REPUTATION-BASED INTERNET PROTOCOL SECURITY: A MULTILAYER SECURITY FRAMEWORK FOR MOBILE AD HOC NETWORKS

DISSERTATION

Timothy H. Lacey, Contractor

AFIT/DCS/ENG/10-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/DCS/ENG/10-07

REPUTATION-BASED INTERNET PROTOCOL SECURITY: A MULTILAYER SECURITY FRAMEWORK FOR MOBILE AD HOC NETWORKS

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

Timothy H. Lacey, B.S., M.S.

Contractor

September 2010

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/DCS/ENG/10-07

REPUTATION-BASED INTERNET PROTOCOL SECURITY: A MULTILAYER SECURITY FRAMEWORK FOR MOBILE AD HOC NETWORKS

Timothy H. Lacey, B.S., M.S.

Contractor

Approved:

Robert F Mills	17 AUG 2010
R.F. Mills, PhD (Chairman)	Date
Barry Mullins	17 Aug 10
B.E. Mullins, PhD (Member)	Date
Richard A Raines	17 Aug 10
R.A. Raines, PhD (Member)	Date
Mark E. Oxley	17 Aug 10
M.E. Oxley, PhD (Member)	Date
	17 Aug 10
S.K. Rogers, PhD (Member)	Date

Accepted:

M U Thomas	26 Aug 10
M. U. Thomas Dean, Graduate School of Engineering and Management	Date

Abstract

This research effort examines the theory, application, and results for a Reputation-based Internet Protocol Security (RIPSec) framework that provides security for an ad-hoc network operating in a hostile environment. In RIPSec, protection from external threats is provided in the form of encrypted communication links and encryption-wrapped nodes while internal threats are mitigated by behavior grading that assigns reputations to nodes based on their demonstrated participation in the routing process. Network availability is provided by behavior grading and round-robin multipath routing.

If a node behaves faithfully, it earns a positive reputation over time. If a node misbehaves (for any number of reasons, not necessarily intentional), it earns a negative reputation. Each member of the MANET has its own unique and subjective set of Reputation Indexes (RI) that enumerates the perceived reputation of the other MANET nodes. Nodes that desire to send data will eliminate relay nodes they perceive to have a negative reputation during the formulation of a route.

A 50-node MANET is simulated with streaming multimedia and varying levels of misbehavior to determine the impact of the framework on network performance. Results of this research were very favorable. Analysis of the simulation data shows the number of routing errors sent in a MANET is reduced by an average of 52% when using RIPSec. The network load is also reduced, decreasing the overall traffic introduced into the MANET and permitting individual nodes to perform more work without overtaxing their limited resources.

Finally, throughput is decreased due to larger packet sizes and longer round trips for packets to traverse the MANET, but is still sufficient to pass traffic with high bandwidth requirements (i.e., video and imagery) that is of interest in military networks.

Acknowledgements

A personal thank you to my wife for her unconditional love during this process. Without her support, completing the degree would not have been possible.

I owe a great dept of gratitude to my advisor, Dr. Robert F. Mills, for his perseverance and patience with me during this journey. We have always worked well together and his mentoring of me was as important as his technical leadership. I am also grateful for my research committee: Dr. Barry E. Mullins, Dr. Richard A. Raines, Dr. Mark E. Oxley, and Dr. Steven K. Rogers for numerous document reviews, feedback sessions, and general support of my research, publications, and this dissertation. Thanks Dr. Raines for the opportunity to pursue this degree while working in our organization.

I must also thank Dr. Rusty O. Baldwin and Mr. Juan Lopez, both whom provided much advice and acted as sounding boards for my ideas. They might as well had been on my committee for all the help they provided. I would never have gotten through the statistics portion of this document had it not been for Juan.

A special thanks to Dr. Nathaniel J. Davis. If not for his encouragement, I may have never started this journey. He made changes to the PhD program that enabled me to see a way through it. Thanks Nat.

Timothy H. Lacey

Table of Contents

Page

Abstract iv

Acknowledgements v

List of Figures xi

List of Tables xiii

List of Abbreviations xv

1. Introduction 1
   - 1.1 Overview 1
   - 1.2 Background 1
   - 1.3 Problem Statement 4
   - 1.4 Approach 4
   - 1.5 Research Contributions 4
   - 1.6 Assumptions/Limitations 5
   - 1.7 Dissertation Organization 6

2. Literature Review 7
   - 2.1 Chapter Overview 7
   - 2.2 MANETs 7
     - 2.2.1 Definition 7
     - 2.2.2 Environment Characteristics 8
     - 2.2.3 Applications 8
     - 2.2.4 Security Considerations 11
   - 2.3 Managing Security in MANETs 13
     - 2.3.1 Behavior Grading 14
     - 2.3.2 IPSec 15
     - 2.3.3 Intrusion Detection Systems 19
   - 2.4 Route Selection 20
     - 2.4.1 Ad-hoc On-demand Distance Vector 20
     - 2.4.2 Dynamic Source Routing 22
     - 2.4.3 Multipath Routing 23
     - 2.4.4 Round-Robin Routing 24
   - 2.5 MANET Security Frameworks 25
     - 2.5.1 MObile Certification Authority 25
     - 2.5.2 Maximum Degree Algorithm 26

Page

2.5.3 Self-Organized Network-Layer Security 26
2.5.4 Techniques for Intrusion Resistant Ad-hoc Routing Algorithms 27
2.5.5 Secure Efficient Ad-hoc Distance Vector 27
2.5.6 On-demand Secure Routing Protocol 27
2.5.7 Alliance of Remote Instructional Authoring and Distributed Networks for Europe 28
2.5.8 Security Aware Ad-hoc Routing 28
2.5.9 Collaborative Reputation Mechanism 29
2.5.10 Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks 29
2.5.11 Watchdog and Pathrater 30
2.6 Trust Management in Ad-hoc Networks 30
2.7 Tying It All Together 33

3. RIPSec Design 35
3.1 Chapter Overview 35
3.2 Design 36
3.2.1 Node Roles 36
3.2.2 Node Formalization 36
3.2.3 Confidentiality and Integrity 38
3.2.4 Reputation and Behavior Grading 41
3.2.5 Routing 46
3.3 Summary 47

4. Simulation Methodology 49
4.1 Chapter Overview 49
4.2 Simulation Environment and Architecture Models 49
4.2.1 Simulation Environment 49
4.2.2 Coefficient of Variation 51
4.2.3 Experimental Design 52
4.2.4 Confidence Interval 52
4.2.5 Analysis of Variance 53
4.3 Simulation Equipment 54
4.4 Metrics for Performance Evaluation and Analysis 54
4.4.1 Total Route Errors Sent 54
4.4.2 Load 54
4.4.3 Throughput 55
4.5 Simulation Model Validation 55
4.5.1 Model Validation Implementation 55
4.5.2 Model Validation Results 56
4.6 Summary 57

Page

5. Simulation Results 58
5.1 Chapter Overview 58
5.2 RIPSec Performance 58
5.3 Diagnostics for Residuals 62
5.3.1 Residuals by Predicted Plot 62
5.3.2 Diagnostics for Residuals Summary 64
5.4 Data Analysis 65
5.4.1 Actual by Predicted Plot 65
5.4.2 Variance Inflation Factors (VIF) 70
5.4.3 Analysis of Variance (ANOVA) 71
5.4.4 Data Analysis Summary 72
5.5 Prediction Expression 73
5.6 Summary 74

6. RIPSec Analysis 75
6.1 Chapter Overview 75
6.2 Engineering Advantages of RIPSec 75
6.3 Effectiveness of RIPSec Against MANET Attacks 76
6.3.1 Eavesdropping 76
6.3.2 Routing Table Overflow 76
6.3.3 Routing Cache Poisoning 77
6.3.4 Routing Maintenance 77
6.3.5 Data Forwarding 77
6.3.6 Wormhole 78
6.3.7 Sinkhole 78
6.3.8 Byzantine 79
6.3.9 Selfish Nodes 79
6.3.10 External Denial of Service 79
6.3.11 Internal Denial of Service 80
6.3.12 Spoofing 80
6.3.13 Sybil 80
6.3.14 Badmouthing 80
6.3.15 Flattering 81
6.4 Comparison of RIPSec to Existing Frameworks 81
6.5 Chapter Summary 81

7. Conclusion 84
7.1 Summary of Research 84
7.2 Research Contributions 84
7.3 Recommendations for Future Research 86
7.4 Concluding Thoughts 87

Page

Appendix A. 88
A.1 IP Dispatch Function Block 88
A.1.1 IP Dispatch Do Init 88
A.1.2 IP Dispatch Init Phase 2 88
A.2 DSR Rte Function Block 88
A.2.1 DSR Rte Sv Init 88
A.2.2 DSR Rte Stats Reg 88
A.2.3 DSR Rte Received Pkt Handle 88
A.2.4 DSR Rte Received Route Error Process 88
A.2.5 DSR Rte Received Acknowledgement Option Process 88
A.2.6 DSR Rte Route Error Send 88
A.2.7 DSR Rte Jittered Pkt Send 88
A.2.8 DSR Rte Route Cache Update 88
A.3 DSR Route Cache 88
A.3.1 Declarations 88
A.3.2 DSR Route Cache Entry Add 88
A.3.3 DSR Route Cache Entry Access 89
A.3.4 DSR Route Cache Path Get 89
A.4 IP Rte Support Header 89
A.4.1 Declarations 89
A.5 DSR Ptypes Header 89
A.5.1 Declarations 89

Appendix B. 90
B.1 AODV Routing Overhead Data for Model Verification . 90
B.2 AODV End-to-End Delay Data for Model Verification . 91
B.3 1 Feedback Node Determination Data 92
B.4 2 Feedback Node Determination Data 93
B.5 3 Feedback Node Determination Data 94
B.6 4 Feedback Node Determination Data 95
B.7 5 Feedback Node Determination Data 96

Appendix C. 98
C.1 Baseline 50 Nodes - 0 Misbehaving 98
C.2 Baseline 50 Nodes - 25 Misbehaving 98
C.3 Baseline 50 Nodes - 5 Misbehaving 98
C.4 RIPSec 50 Nodes - 0 Misbehaving 99
C.5 RIPSec 50 Nodes - 25 Misbehaving 99
C.6 RIPSec 50 Nodes - 5 Misbehaving 99
C.7 Baseline 25 Nodes - 0 Misbehaving 100

Page

C.8 Baseline 25 Nodes - 12 Misbehaving 100
C.9 Baseline 25 Nodes - 2 Misbehaving 100
C.10 RIPSec 25 Nodes - 0 Misbehaving 101
C.11 RIPSec 25 Nodes - 12 Misbehaving 101
C.12 RIPSec 25 Nodes - 2 Misbehaving 101

Bibliography 102

List of Figures

Figure		Page
1.1.	A Large-scale Deployment of Autonomous Teams in a MANET [9]	2
2.1.	Multihop MANET [61]	8
2.2.	DARPA's First-Generation MANET Network Architecture [44]	10
2.3.	Peer-to-Peer MANET Architecture [37]	11
2.4.	Trust-based Recommendation Scenario [29]	14
2.5.	IPSec Component Interaction [22]	16
2.6.	Synopsis of IPSec Modes and Protocols [77]	17
2.7.	Security-guaranteed Trusted Group [61]	19
2.8.	AODV Protocol Messaging	21
2.9.	DSR Route Discovery	22
2.10.	Multipath Routing	23
2.11.	Trust Management System Architecture [1]	32
3.1.	RIPSec MANET Components	36
3.2.	Multiple Paths in a RIPSec MANET	37
3.3.	Security Associations Between Nodes	39
3.4.	Transmitting Data	40
3.5.	RIPSec Feedback Items	44
3.6.	Negative Reputation Node Participation	44
4.1.	Routing Overhead in AODV	57
4.2.	End-to-End Delay in AODV	57
5.1.	Analysis of Errors Sent By Group	59
5.2.	Analysis of Load By Group	60
5.3.	Analysis of Throughput By Group	61
5.4.	Errors Sent Residual by Predicted Plot	63
5.5.	Load Residual by Predicted Plot	64

Figure Page

5.6. Throughput Residual by Predicted Plot 64

5.7. Example Actual by Predicted Plot 66

5.8. Actual by Predicted Plot for Errors Sent 68

5.9. Actual by Predicted Plot for Load 69

5.10. Actual by Predicted Plot for Throughput 70

5.11. Variance Inflation Factors 71

5.12. ANOVA for Errors Sent 72

5.13. ANOVA for Load 72

5.14. ANOVA for Throughput 73

6.1. RIPSec Comparison to Existing Frameworks Part 1 82

6.2. RIPSec Comparison to Existing Frameworks Part 2 83

List of Tables

Table		Page
3.1.	Feedback Nodes Metrics	46
4.1.	OPNET Simulation Parameters	50
4.2.	RIPSec Factors and Levels	51
4.3.	RIPSec Factor Level Combinations	52
4.4.	Validation Workload Parameter Settings [60]	56
5.1.	Simulation Groups	58
5.2.	Percentage Change in Errors Sent By Group	59
5.3.	Percentage Change in Load By Group	60
5.4.	Percentage Change in Throughput By Group	60
5.5.	Goodness-of-Fit Test (Shapiro-Wilk W Test)	65
5.6.	Individual Factors' P-values for Errors Sent	68
5.7.	Individual Factors' P-values for Load	69
5.8.	Individual Factors' P-values for Throughput	70
7.1.	RIPSec Areas of Improvement	86
B.1.	AODV Routing Overhead Data for Model Verification	90
B.2.	AODV End-to-End Delay Data for Model Verification	91
B.3.	1 Feedback Node Determination Data	92
B.4.	2 Feedback Nodes Determination Data	93
B.5.	3 Feedback Nodes Determination Data	94
B.6.	4 Feedback Nodes Determination Data	95
B.7.	5 Feedback Nodes Determination Data	96
B.8.	6 Feedback Nodes Determination Data	97
C.1.	Baseline 50 Nodes - 0 Misbehaving	98
C.2.	Baseline 50 Nodes - 25 Misbehaving	98
C.3.	Baseline 50 Nodes - 5 Misbehaving	98

Table Page

C.4. RIPSec 50 Nodes - 0 Misbehaving 99

C.5. RIPSec 50 Nodes - 25 Misbehaving 99

C.6. RIPSec 50 Nodes - 5 Misbehaving 99

C.7. Baseline 25 Nodes - 0 Misbehaving 100

C.8. Baseline 25 Nodes - 12 Misbehaving 100

C.9. Baseline 25 Nodes - 2 Misbehaving 100

C.10. RIPSec 25 Nodes - 0 Misbehaving 101

C.11. RIPSec 25 Nodes - 12 Misbehaving 101

C.12. RIPSec 25 Nodes - 2 Misbehaving 101

List of Abbreviations

Abbreviation		Page
MANET	Mobile Ad-hoc Network	1
DoS	Denial of Service	1
UAV	Unmanned Aerial Vehicles	2
RPV	Remotely Piloted Vehicle	2
IDS	Intrusion Detection Systems	3
RIPSec	Reputation-based Internet Protocol Security	4
USB	Universal Serial Bus	5
OPNET	Optimized Network Engineering Tools	5
IPSec	Internet Protocol Security	7
TCP	Transmission Control Protocol	8
DARPA	Defense Advanced Research Projects Agency	9
NCRS	Network Centric Radio System	9
RISED	Rescue Information System for Earthquake Disasters	9
ISO	International Organization for Standardization	11
PKI	Public Key Infrastructure	15
IETF	Internet Engineering Task Force	15
AH	Authentication Header	15
ESP	Encapsulating Security Payload	15
OS	Operating System	16
DOI	Domain of Interpretation	17
ISAKMP	Internet Security Association and Key Management Protocol	17
SA	Security Association	17
DES	Data Encryption Standard	18
HMAC-SHA	Hash-based Message Authentication Code - Secure Hash Algorithm	18

Abbreviation		Page
SADB	SA DataBase	18
SPD	Security Policy Database	18
AODV	Ad-hoc On-demand Distance Vector	20
DSR	Dynamic Source Routing	20
RREQ	Route Request	21
RREP	Route Reply	21
RERR	Route Error	22
SMR	Split Multipath Routing	24
MSR	Multipath Source Routing	24
MOCA	MObile Certification Authority	25
CA	Certificate Authority	25
MDA	Maximum Degree Algorithm	26
SCAN	Self-Organized Network-Layer Security	26
TIARA	Techniques for Intrusion Resistant Ad-hoc Routing Algorithms	27
SEAD	Secure Efficient Ad-hoc Distance Vector	27
OSRP	On-demand Secure Routing Protocol	27
ARIADNE	Alliance of Remote Instructional Authoring and Distributed Networks for Europe	28
SAR	Security Aware ad-hoc Routing	28
CORE	Collaborative Reputation Mechanism to Enforce Node Cooperation	29
CONFIDANT	Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks	29
KMS	Key Management System	30
TMS	Trust Management System	31
FI	Feedback Item	31
IKE	Internet Key Exchange	38
SHA-1	Secure Hash Algorithm 1	39

Abbreviation		Page
MD5	Message Digest 5	39
NS2	Network Simulator 2	49
C.O.V.	Coefficient of Variation	51
ANOVA	Analysis of Variance	53
MAC	Medium Access Control	54
VIF	Variance Inflation Factors	65
ANOVA	Analysis of Variance	65
RSq	RSquare	67
RMSE	Root Mean Square Error	67
DF	Degrees of Freedom	71
RF	Radio Frequency	76

REPUTATION-BASED INTERNET PROTOCOL SECURITY: A MULTILAYER SECURITY FRAMEWORK FOR MOBILE AD HOC NETWORKS

1. Introduction

1.1 Overview

Mobile Ad-hoc Networks (MANET) are self-configuring networks of mobile routers connected by wireless links [31]. When one node desires to communicate with another that is out of transmission range, intermediate nodes are used to relay messages [13]. There are many security issues to be concerned with in this type of communication scheme. The main considerations for MANET security are confidentiality, integrity, availability, authorization, dependability, reliability, and accountability [89]. External threats include passive eavesdropping and active interference. Internal threats consist of failed nodes, selfish nodes, and malicious nodes. Some of the many attacks that malicious nodes can launch are Denial of Service (DoS) attacks, attacks on network integrity, attacks on neighbor sensing protocols, misdirecting traffic, exploiting route maintenance, attacking sequence numbers, and attacks on protocol specific optimizations. The use of firewalls and encryption algorithms can help tremendously to protect nodes from external threats. Internal threats can be mitigated by a behavior grading scheme that assigns reputation values to each node and refrains from using nodes that misbehave. To help ensure routes are available from sender to receiver nodes, round-robin multipath routing algorithms provide necessary network resources required to support high bandwidth applications.

1.2 Background

MANETs have received the attention of numerous agencies due to their self-configuration and self-maintenance capabilities. Their many applications include mil-

itary battlefields, disaster relief efforts, conferences, classrooms, taxicabs, sports stadiums, boats, and small aircraft [78]. In [9], Unmanned Aerial Vehicles (UAVs) are organized into MANETs to facilitate intra-team communications. Additionally, Figure 1.1 shows how teams of MANETs composed of several military components, to include UAVs, may be organized and deployed.

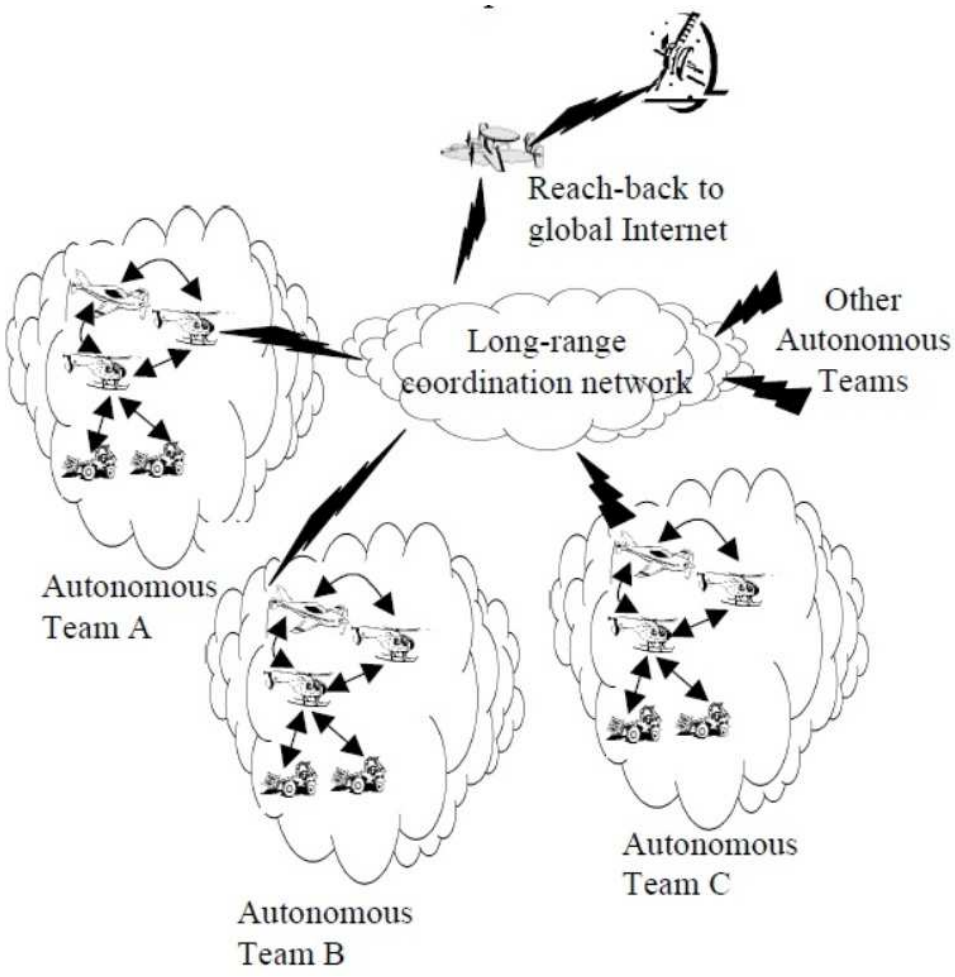

Figure 1.1: A Large-scale Deployment of Autonomous Teams in a MANET [9]

Live surveillance video is increasingly in demand on the battlefield to achieve information dominance [18]. Remotely Piloted Vehicles (RPVs) are currently being formulated and fielded at a breathtaking pace, some of them no bigger than paper planes [8]. State-of-the-art video compression and transmission technology will be needed to achieve real-time transmission of the on-board sensors.

Early MANET research efforts focused on functionality [86]. Security has now become a priority since MANETs are being deployed in potentially hostile environments [87]. Traditional wired security solutions do not apply to MANETs due to their "open" network architecture (nearby nodes will often be capable of sending and receiving MANET protocol packets), shared wireless medium, resource constraints, and dynamic network topology. For a MANET to be secure, required services include authentication, confidentiality, integrity, availability, and non-repudiation. Any security solution that provides these services must be implemented at each level of the communications stack, commonly divided into three major sections: media, transport, and applications [14].

A unique characteristic of MANET security is the lack of a clear line of defense. Traditional fixed networks have dedicated infrastructure such as firewalls, routers, and Intrusion Detection Systems (IDS) to provide protection from outside threats. However, each MANET node functions as its own router and forwards packets to other peer nodes. The wireless channel used by a MANET is open to both legitimate users, eavesdroppers, and malicious attackers. No well-defined place exists in a MANET where traffic can be monitored or access control deployed. Therefore, there is no clear separation between the "inside" and "outside" network. Since there is no clear threat to defend against, typical MANET routing protocols assume a trusted and cooperative environment. This blind trust enables malicious nodes to disrupt network operations by intentionally disobeying protocol specifications. Nodes may also misbehave unintentionally due to hardware failure or restriction of resources, such as limited battery power.

MANET protection techniques can be classified as proactive or reactive. Proactive approaches use various cryptographic techniques to prevent an attacker from launching attacks while reactive techniques attempt to detect security threats after they occur and react appropriately. Any complete security solution for MANETs should include prevention, detection, and reaction.

1.3 Problem Statement

This research investigates how to integrate security policies of a MANET with behavior grading and encryption algorithms in a fashion that will allow the MANET to function securely in a hostile environment without degrading network performance. The specific problem to be addressed is how to use behavior grading of nodes in a multipath routing algorithm to control security mechanisms (e.g., encryption algorithms) and provide a MANET capable of supporting high bandwidth applications (e.g., video and imagery) that is protected from both internal and external threats.

1.4 Approach

The approach taken to solve this research problem is as follows:

- Design and define the proposed framework, Reputation-based Internet Protocol Security (RIPSec)
- Validate the RIPSec framework through modeling and simulation
- Analyze RIPSec's performance through simulation
- Assess and show the engineering advantages of using RIPSec over other well-known MANET security frameworks

1.5 Research Contributions

Reputation-based Internet Protocol Security (RIPSec) is a framework created through this research for integrating multipath routing with encryption algorithms and security policies via node behavior grading in a MANET. It provides a system in which high bandwidth applications can operate securely in a tactical, contested environment. Previous research in this area focused on extending ad-hoc network protocols to address either security or application concerns. There has been little research performed that integrates multipath routing protocols with encryption and behavior grading mechanisms due to the limited resources of MANET nodes, limited

bandwidth of wireless channels, and generally hostile transmission characteristics of wireless mediums [16]. This framework will demonstrate how to deploy a MANET with: 1) encryption technologies to secure communications while uniquely identifying each node, 2) a behavior grading mechanism to isolate nodes with poor reputations, and 3) a round-robin multipath routing algorithm that provides necessary network resources for high bandwidth applications.

1.6 Assumptions/Limitations

The use of encryption algorithms to secure communication between nodes is mandatory. Nodes will utilize digital certificates for identification and as keys for the encryption algorithms. Each node's public key will be distributed using an external means of communication (e.g., a Universal Serial Bus (USB) device) to all other nodes before deployment of the MANET. A collaborative reputation mechanism will be used to assign reputation indices to nodes [54]. A multipath algorithm will be used to provide routes between sender and receiver nodes. The framework will be simulated using the Optimized Network Engineering Tools (OPNET) discrete event simulator, version 15.0. The following metrics will be analyzed in the MANET and in the nodes.

- Load
- Throughput
- Total Route Errors Sent

Video conferencing with a medium workload was used to demonstrate the feasibility of the framework [75]. Due to the size of the network (50 nodes), the mobility of the nodes (random waypoint at 0 - 10 meters per second), and node misbehavior (0 - 40%), it was not feasible to implement the framework in a test bed at this time.

1.7 Dissertation Organization

This dissertation is organized as follows. Chapter 2 contains a review of seminal and recent publications providing necessary information pertaining to the research problem. Chapter 3 describes the development of the RIPSec framework. Chapter 4 describes the methodology for validating/verifying the RIPSec framework, and Chapter 5 presents simulation results. Chapter 6 discusses the advantages of RIPSec over other reputation-based methods of managing MANETs. Finally, Chapter 7 concludes the dissertation and presents areas for further study.

2. Literature Review

2.1 Chapter Overview

This chapter provides an overview of background knowledge and relevant existing literature for the proposed research problem. Section 2.2 provides an overview of MANETs, examples of how they are used, and methods/issues associated with monitoring/managing the network. Section 2.3 addresses various methods used to manage security in a MANET, specifically, behavior grading, Internet Protocol Security (IPSec), and Intrusion Detection Systems. Section 2.4 reviews several published MANET security frameworks, and Section 2.5 explains selection of routes from sender to receiver in a MANET. Section 2.6 discusses the role of trust in ad-hoc networks. Section 2.7 summarizes the chapter.

2.2 MANETs

MANETs are mobile wireless communication systems that may be formed without any pre-existing infrastructure. The following subsections provide further details.

2.2.1 Definition. A MANET is "an autonomous system of routers and associated hosts/nodes connected by wireless links, the union of which forms an arbitrary graph" [35].

MANET nodes are transitive and change the network's topology dynamically as they join and leave the network unpredictably. An example of a multihop MANET is shown in Figure 2.1. The sender node uses a dynamic route through relay nodes to send data to the receiver node. As nodes move, the route may change. There may be several routes from sender to receiver, but often only one route is used in a MANET between sender and receiver nodes.

Since a MANET does not require a traditional infrastructure, it can be deployed quickly in a variety of applications. The military, disaster relief organizations, expeditionary forces, and the media are all potential users of MANETs.

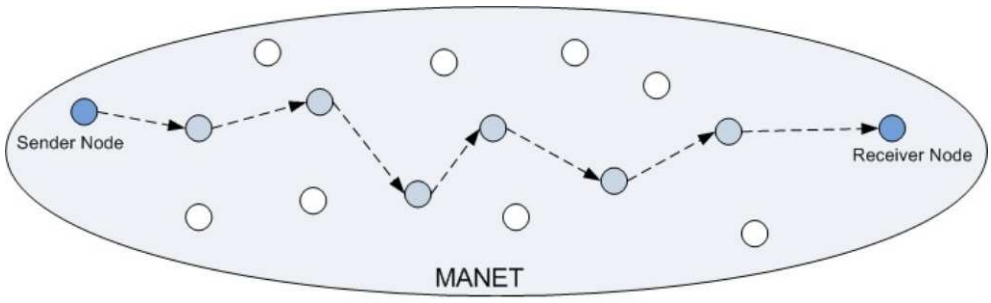

Figure 2.1: Multihop MANET [61]

2.2.2 Environment Characteristics. MANETs require cooperation among nodes to provide the various services necessary for the network to operate. Since the links in a MANET are wireless, there are bandwidth limitations, and these links experience a higher probability of data error than if operating on wired links. The malfunctioning of one or more links along a certain route requires the retransmission of all packets from the originating sender node, assuming a connection-based protocol such as Transmission Control Protocol (TCP). This unnecessary amount of retransmission results in significant overhead that can severely degrade the overall network performance by increasing the average time delay of packet delivery [71]. This has the net effect of decreasing the rate of information transfer. Software that handles traffic on the nodes must be aware of the congestion possibilities and the high data error rates that could occur. If the MANET topology is very dynamic, routing changes need to propagate quickly to avoid extensive data loss. MANET nodes are often battery powered, potentially limiting their functionality and processing capabilities within the network. When battery power is too low, the wireless range may be reduced and nodes may not be able to transmit/receive packets. Some applications of MANETs are discussed next.

2.2.3 Applications. MANETs are typically used when there is little to no communication infrastructure. They can also be used where the existing infrastructure is too expensive or inconvenient to use. Applications that use MANETs vary between large-scale, mobile, highly dynamic networks and small, static networks

constrained by power sources [78]. Additionally, MANETs have varied missions, implementations, and operational requirements. A few examples are summarized in the following subsections.

2.2.3.1 Military Battlefield. Information technology is increasingly prevalent in the modern battlefield. MANETs allow the military to use mobile network technology to maintain connectivity between soldiers, vehicles, and information headquarters [62]. In [44], The Defense Advanced Research Projects Agency's (DARPA's) Network Centric Radio System (NCRS) is a first-generation MANET designed to enable ground and airborne-vehicle-based on-the-move and on-the-halt network-centric connectivity. NCRS offers interoperability among various current, future, coalition, and first responder communications radios via the network. One of the most challenging aspects of a military MANET is the use of mixed node types. As shown in Figure 2.2, these networks operate and interface between unattended ground sensors, pedestrians, ground vehicles, low altitude aircraft, ships, high altitude aircraft, and satellite platforms. Each has different characteristics in mobility, available power, line-of-sight, and latency tolerance. They also have different networking requirements, placing challenges on the interfaces between them.

2.2.3.2 Commercial Sector. Emergency rescue operations for disaster relief efforts such as fire, flood, and earthquakes are appropriate applications for MANETs [79]. Often, these operations take place where non-existing or damaged communications infrastructure exists and rapid deployment of a communications network is needed. Information is relayed from one rescue unit to another via a hand held device or node [78]. In [37], the Rescue Information System for Earthquake Disasters (RISED) is designed to support a more efficient rescue and relief operation for catastrophic earthquakes. The objective of RISED is to provide the most up-to-date and accurate rescue-related information possible, such as disaster locations, possible damages to both lives and constructions, available rescue and relief resources, and the shortest way to the disaster spots. A two-tier architecture supports a command post

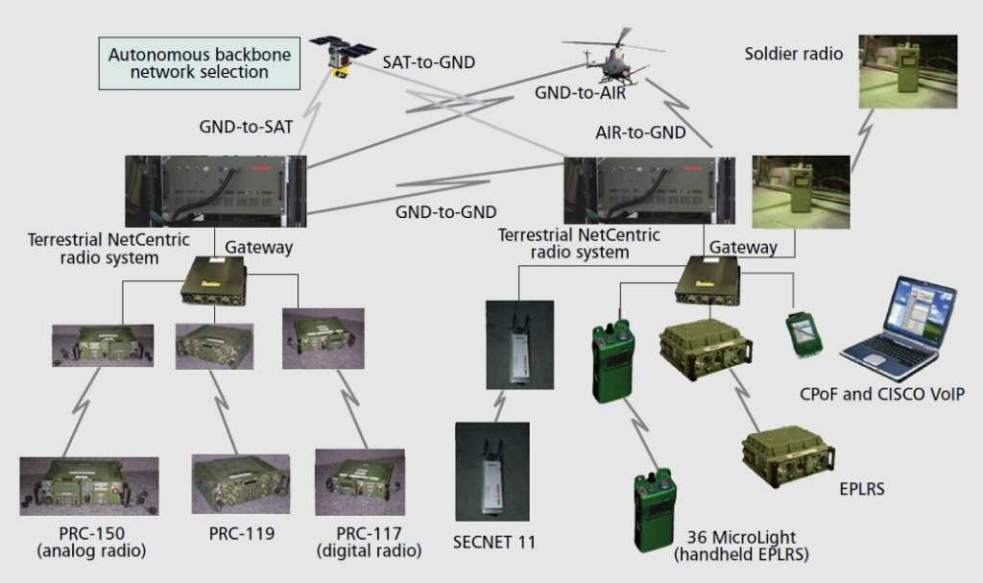

Figure 2.2: DARPA's First-Generation MANET Network Architecture [44]

with the first tier and local deployments with the second tier. If external network connectivity is lost, local deployments can independently operate to help rescue and relief operations. Figure 2.3 illustrates a MANET-based peer-to-peer network used to support RISED.

2.2.3.3 Tactical UAVs. Tactical UAVs are aircraft with greater endurance and payload capacity than smaller "micro" UAVs [3]. These two features often determine when a tactical UAV will be utilized. Tactical UAVs are lower in cost than larger platforms like "Global Hawk" [5] and "Predator" [81]. Examples of tactical UAVs include the "MQ-5B Hunter" and the "RQ-7B Shadow" [72]. Both are designed to gather battlefield reconnaissance, surveillance, target acquisition, and battle damage information in real time using a multi-mission optical payload, then relaying it via video link to commanders and soldiers on the ground. Improvements to the "Shadow" have allowed it to accommodate a communications relay package, which allows the aircraft to act as a relay station and participate in tactical MANETs. Though traditionally resource constrained, research is currently underway to incorporate tactical UAVs into the battlefield [70].

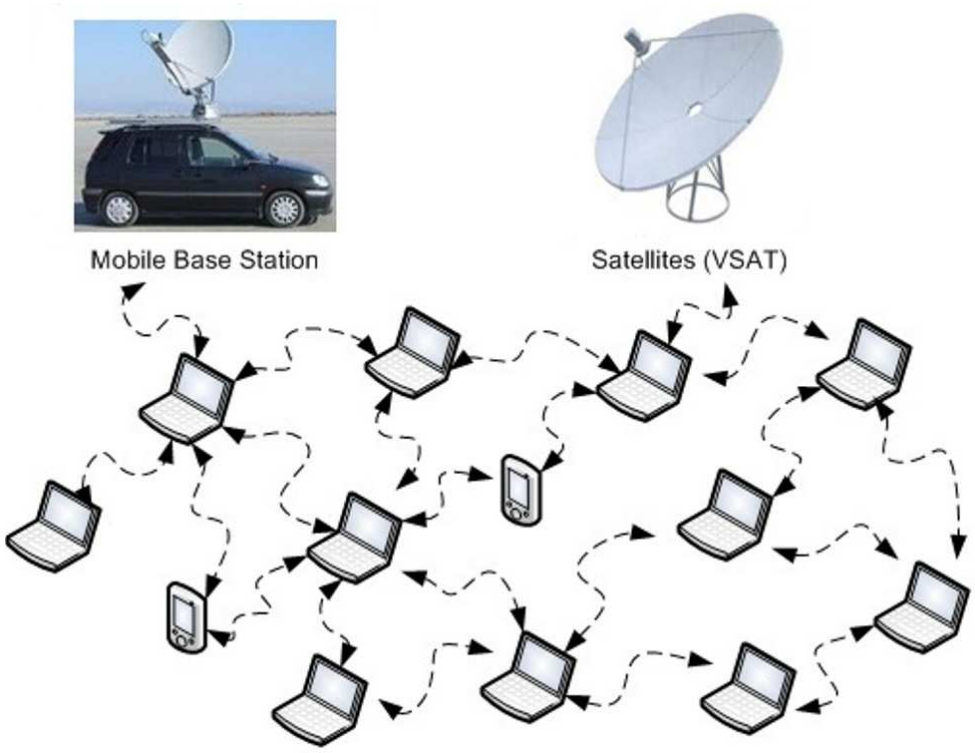

Figure 2.3: Peer-to-Peer MANET Architecture [37]

2.2.4 Security Considerations. Security is very important in communication networks, but perhaps more so in MANETs because they are so easily eavesdropped and there are no infrastructure devices such as firewalls in place to protect the nodes. MANET nodes depend on each other to provide security for the network. In addition to the functional challenges of operating a MANET, many security risks must be addressed. To be secure, a network must provide *confidentiality*, *authentication*, *integrity*, *non-repudiation*, and *availability* as well as physical security [92].

Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security [38]. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography. MANETs can suffer from multiple points

of attack as eavesdroppers may obtain the data transferred without being in the path of traffic.

Authentication is the act of establishing or confirming that claims made by or about something or someone are true. This might involve confirming the identity of a person, the origins of an object, or assuring that a computer program is trusted. A lack of authentication in a MANET can allow an adversary to masquerade as a node, gain access to unauthorized information, and interfere with the operation of the network [26].

Integrity comprises perceived consistency of actions, values, methods, measures, and principles. Applied to MANETs, integrity ensures a transferred message is not corrupted while in transit between the sender and receiver nodes [86].

Non-repudiation is the concept of ensuring that a party cannot refute taking part in a transaction. Although this concept can be applied to any transmission of data, the most common application is in the verification and trust of signatures. Non-repudiation is important to a behavior grading mechanism in MANETs so appropriate grading actions can be accurately assessed and to isolate attackers or compromised nodes [85].

Availability is the degree to which a system, subsystem, or service is operable and ready for use when it is needed. Simply put, availability is the proportion of time a system or service is in a functioning condition. MANETs are vulnerable to DoS attacks, such as electronic jamming, attacks on the routing protocols, and attacks on key management systems, all of which can disrupt trust relationships and disconnect the entire network [52].

Since MANET nodes are mobile, they are not likely to have physical protection in hostile environments. If a MANET node provides a central service and that node is compromised, the entire network may be deprived of that service. Every node in a MANET is a potential victim of compromise. Therefore, the MANET must be able to discern if a particular node has been compromised and effectively mitigate it.

A thorough review of current security strategies indicates that researchers typically use three strategies to mitigate the effects of compromised nodes: trust and behavior grading schemes, authentication and encryption, and intrusion detection systems, all of which are described in the next section. As with most engineering problems, there are tradeoffs between the resource constraints, performance, scalability, and provision of security features. Furthermore, there is no single scheme that provides a general solution for the different types of security threats in the mobile computing environment [45]. Therefore, a hybrid approach that draws upon these security mechanisms is warranted.

2.3 Managing Security in MANETs

Trust and reputation are separate but related concepts. Both are needed to provide an environment that is robust and resistant to attack. In [1], trust and reputation are differentiated, as follows:

> Trust is active; it is a node's belief in the trust qualities of a peer. Trust is extended from a node to its peer. Reputation is passive; it is the perception that peers form about a node. Reputations are individual in the sense that peers can form different reputations about the same node, based on the fact that they can have different experiences or observe different behavior [1].

Grandison [29] says "Trust is the quantified belief by a truster with respect to the competence, honesty, security, and dependability of a trustee within a specified context." Li [50] states that trust is a notation of human behavior. As illustrated in Figure 2.4, a truster (or truster node) refers to the node that implements the trust evaluation. Trustee (or trustee node) refers to the node that is evaluated. A third party node is one that a truster expects who can provide an honest recommendation on a specific trustee [50].

The following section describes how trust is earned and reputations are gained through behavior grading systems in a MANET.

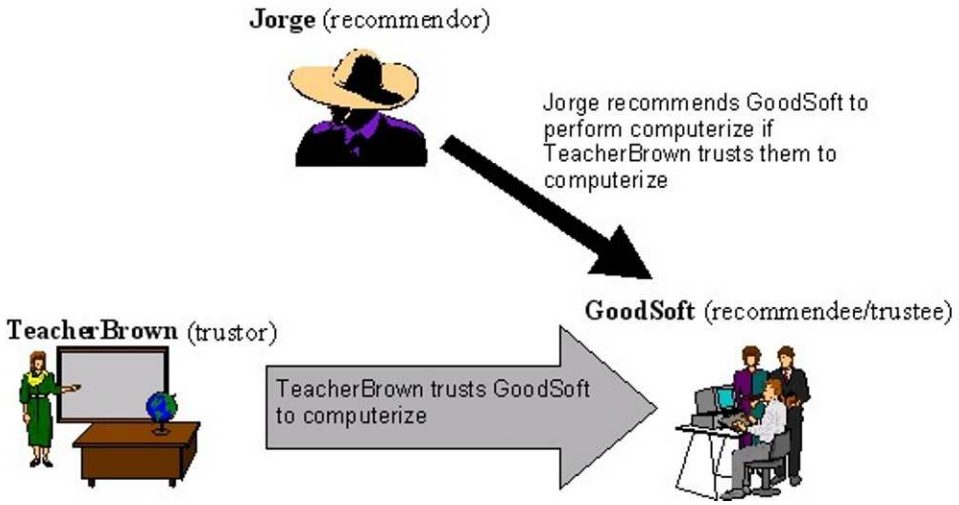

Figure 2.4: Trust-based Recommendation Scenario [29]

2.3.1 Behavior Grading. A variety of environments and applications have motivated research in behavior grading systems [56]. Peer-to-peer eCommerce applications such as eBay, Amazon, uBid, and Yahoo have performed research that indicates reputation systems facilitate fraud avoidance and better buyer satisfaction [32]. Though behavior grading systems have numerous applications, this research focuses on its benefit to MANET security.

According to [54], MANET nodes can be considered members of a community that share a common resource, the network. Nodes exhibit *desirable* behavior when contributing to the community by participating in the route selection process and relaying packets between sender and receiver nodes, and *undesirable* behavior when they do not contribute, whether maliciously or not. The manner in which a node behaves causes it to acquire a reputation, which is a good mechanism to measure the contribution of a particular node to the community. Reputation can be defined as "...the amount of trust inspired by a particular member of a community in a specific setting or domain of interest" [54]. If a particular node behaves in a manner that is beneficial to the network, other nodes will place more trust in that node. The more a node is trusted, the better its reputation. Conversely, if a node's actions are

disruptive or detrimental to the community, then other nodes will trust it less, and its reputation will suffer accordingly.

A node's reputation determines if other nodes in the community will communicate with it. Nodes with a good reputation can use the community's resources while those with bad reputations are gradually excluded from the network [54]. With such consequences at stake, a node's reputation must be determined through careful and thorough analysis that takes into account legitimate reasons why a node may not be contributing to the community, as in the case of dwindling energy resources [54].

As stated in [2], any reputation management system must link a node's identity with its reputation. This is necessary to track the source of behavior feedback and provide non-repudiation of behavior grading. Contrary to Oguchi in [61], this can best be accomplished using a distributed Public Key Infrastructure (PKI) scheme to identify each node [12] [19] [27]. An alternative to using PKI is to use symmetric keys, otherwise known as pre-shared keys. However, the use of pre-shared keys introduces key management problems. For the proposed framework, PKI is preferred because every node is quickly identifiable by its certificate.

While evaluating a node's reputation can help protect a MANET from insider threats, it is not sufficient. External threats necessitate the use of more stringent protection techniques. Traditionally, the Internet Engineering Task Force (IETF) IPSec protocol suite does a very good job protecting wired networks [42]. As presented in the next section, IPSec can also protect MANETs.

2.3.2 IPSec. IPSec is a suite of protocols for protecting IP datagrams [64].

> The set of security services that IPSec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality [42].

It uses two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP) to provide traffic security. The AH protocol provides connectionless in-

tegrity, data origin authentication, and an optional anti-replay service while the ESP protocol may provide confidentiality (encryption) and limited traffic flow confidentiality in addition to the features provided by the AH protocol. The two protocols may be used separately or in conjunction with each other. However, it is only necessary to use the ESP protocol since it provides all the capabilities of the AH protocol and more.

2.3.2.1 Architecture. The IPSec architecture defines the capabilities the network nodes and gateways should provide. Depending on the security requirements of the users, IPSec can be implemented and deployed in the end nodes or the gateways/routers or in both. In the node implementation, IPSec may be integrated with the Operating System (OS). Additionally, since IPSec is a network layer protocol, it may be implemented as part of the network layer. The gateway/router implementation provides the ability to secure packets over a portion of the network, such as the public Internet connection between two geographically separated buildings of an organization. Figure 2.5 demonstrates how the various components of IPSec interact with each other. A user chooses either the ESP or AH protocol to protect the connection. If ESP is chosen, the connection is encrypted and authenticated. If AH, the connection is only authenticated.

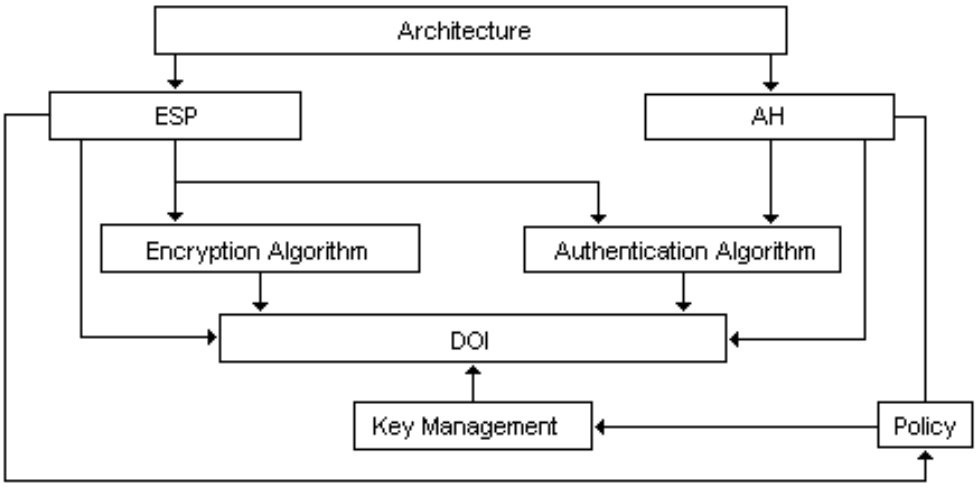

Figure 2.5: IPSec Component Interaction [22]

The IPSec Domain of Interpretation (DOI) serves to group related protocols using the Internet Security Association and Key Management Protocol (ISAKMP) to negotiate Security Associations (SA) [22]. However, before SAs can be established, an IPSec connection mode must be determined.

2.3.2.2 Connection Modes. IPSec has two types of connection modes, tunnel and transport. Tunnel mode is established between two gateways, a gateway and a node, or between two nodes. It creates an encrypted tunnel between the endpoints, adding a new IP header to the original packet [4]. Transport mode is strictly a node to node connection where all the data between the two nodes is encrypted. As illustrated in Figure 2.6, the major difference between the two modes is that the entire original IP packet is encrypted in tunnel mode whereas the IP packet header is not encrypted in transport mode. Additionally, if the ESP protocol is used, each packet contains trailer and authentication data.

Transport Mode with AH					
	IP Header	AH Header	TCP/UDP/ICMP Payload		
Transport Mode with ESP					
	IP Header	ESP Header	TCP/UDP/ICMP Payload	ESP Trailer	Authentication Data
No Encryption					
		IP Header	TCP/UDP/ICMP Payload		
Tunnel Mode with AH					
New IP Header	AH Header	IP Header	TCP/UDP/ICMP Payload		
Tunnel Mode with ESP					
New IP Header	ESP Header	IP Header	TCP/UDP/ICMP Payload	ESP Trailer	Authentication Data

Figure 2.6: Synopsis of IPSec Modes and Protocols [77]

2.3.2.3 Security Associations. An SA is the contract between two communicating nodes. It determines the protocols used for securing packets, transforms, encryption keys, and the duration for which the encryption keys are valid.

A transform describes a security protocol (AH or ESP) with its corresponding algorithms. For example, ESP with the Data Encryption Standard (DES) cipher algorithm and Hash-based Message Authentication Code - Secure Hash Algorithm (HMAC-SHA) for authentication. IPSec SAs are stored on each node in an SA DataBase (SADB). SAs work in only one direction, either inbound or outbound. Therefore, if two nodes, A and B, are communicating securely, then node A will have an SA, *SAout*, for processing outbound packets and a second SA, *SAin*, for processing inbound packets [22]. Additionally, node B will create two SAs for processing its packets. The *SAout* of node A and the *SAin* of node B will share the same cryptographic parameters (keys). Similarly, the *SAin* of node A and the *SAout* of node B will share the same cryptographic parameters. Because SAs are unidirectional, a separate table must be maintained for SAs used for outbound and inbound processing. There is an SA for each IPSec protocol. If two nodes A and B are communicating securely using both AH and ESP, then each node builds a separate SA for each protocol. To minimize the amount of memory required by each node to maintain SAs, only one protocol (AH or ESP) is typically used. ESP provides the most capability and is usually recommended [74].

Every node using IPSec maintains a Security Policy Database (SPD). The SPD works in conjunction with the SADB in processing packets. The security policy defines the security communications characteristics between two communicating nodes. It defines what protocols to use in what modes, the transforms to use, and how the IP packets are treated. Without a security policy, an SA cannot exist. Figure 2.7 illustrates how only nodes with the proper SAs can communicate with the other nodes in the secured MANET.

If configured correctly, IPSec security associations create a formidable barrier against unauthorized users. MANETs deployed without encryption mechanisms like IPSec often depend on Intrusion Detection Systems to identify malicious behavior. These systems are reviewed in the next section.

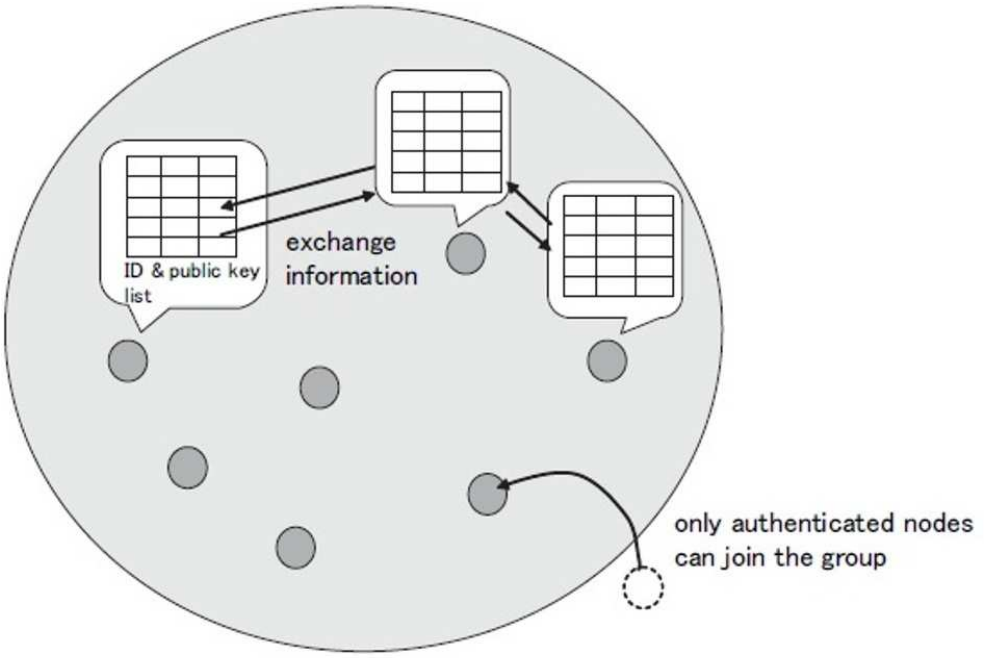

Figure 2.7: Security-guaranteed Trusted Group [61]

2.3.3 Intrusion Detection Systems. According to [6], "An Intrusion Detection System (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device. It is not a stand-alone protection measure." IDSes can be classified into three categories: 1) Signature-based 2) Anomaly-based, and 3) Specification-based [40].

Signature-based IDSes compare pre-defined signatures of known attack scenarios to incoming packet streams, alerting users of attacks [40]. Various approaches to signature-based attacks include expert systems [53], pattern recognition [23], colored Petri Nets [46], and state transition analysis [66]. Anomaly-based IDSes attempt to detect patterns of activity that deviate from "normal" expected system behavior [6]. Statistics [67], neural networks [20], immunology [25], data mining [49] [24], and chi-square test utilization [17] are all approaches used in anomaly-based IDSes. Specification-based IDSes are a hybrid of the signature and anomaly-based IDS [40].

Specification-based IDSes alert users when a mismatch occurs between current behavior and the system specifications [43].

The problem with the IDS techniques in the previous paragraph is that they are not able to derive generalized solutions to new problems. They only work when observed behavior matches a pattern previously identified as "bad", as in the case of signature-based IDSes, or a known "good", as in the case of anomaly detection techniques. If the observed behavior cannot be classified as "bad" or "good", the IDS must then default to a predetermined response or produce a statistically-based guess. The IDS has no ability to rationalize or deduce the proper action to take when unknown activity is detected. Research has shown that these types of IDSes can be undermined and rendered not only ineffective, but harmful as they can allow the user to believe all is safe and well in the face of attacks [80]. IDSes are not a part of the proposed framework in this research because the focus is to make routing decisions based solely on factual information. Acknowledgments and errors generated by the routing protocol will be used exclusively in this framework.

2.4 Route Selection

Proactive routing protocols generate routes and store them for later use. On-demand routing protocols only generate routes when necessary. The latter is used more often in MANETs because they require fewer resources. Two of the more popular on-demand routing protocols are Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) [7]. Unless modified, both of these protocols use single routes between sender and receiver nodes. Multipath routing reduces dependency on single nodes and routes, offering robustness in a secured MANET. The following sections provide a description of these protocols.

2.4.1 Ad-hoc On-demand Distance Vector. In the AODV protocol [15], *Hello* or similar messages are used to discover and monitor links to neighboring nodes. Figure 2.8 shows the message exchanges of the AODV protocol [15]. Each active node

periodically broadcasts a *Hello* message that all neighboring nodes receive. If a node fails to receive several *Hello* messages from a particular neighboring node, a break in the link is assumed.

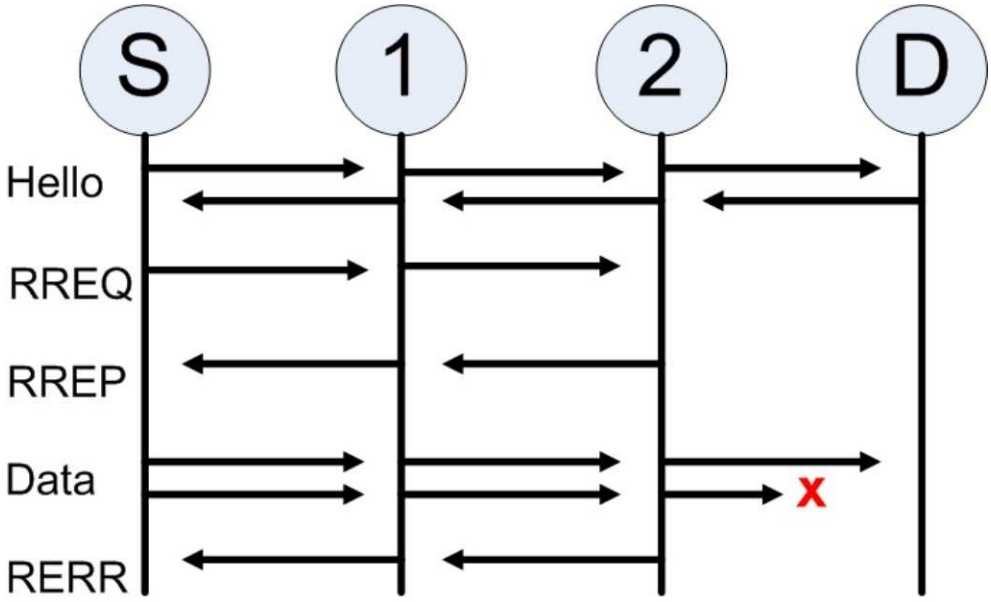

Figure 2.8: AODV Protocol Messaging

When a sender node (node S in Figure 2.8) has data to send to a receiver (node D), it broadcasts a Route Request (RREQ) for the receiver node. When an RREQ is received by an intermediate node (node *1*), a route back to the source is created. If the intermediate node has not received this RREQ before, is not the receiver node, and does not have a current route to the receiver node, it rebroadcasts the RREQ. If a subsequent node is the receiver (node D) or has a current route to the receiver (such as node *2*), it generates a Route Reply (RREP). The RREP is unicast hop-by-hop back to the source. As the RREP propagates, each intermediate node creates a route to the receiver and updates its own routing table. When the sender node receives the RREP, it records the route to the receiver node and begins sending data to it. If the sender node receives multiple RREPs, the route with the shortest hop count is selected.

Each node maintains its own routing table. As data flows from the sender node to the receiver node, each node in the route updates timers associated with the route in its routing table. If a route in the table is not used for a specified amount of time, it is assumed to be invalid and purged from the routing table [15].

Whenever a break in a route is detected, a Route Error (RERR) message is sent to the sender node of the data stream. As the RERR message works its way back to the sender node, each intermediate node in the route updates its routing table to purge routes using the unreachable node. When the sender node of the data stream receives the RERR message, it invalidates the route currently being used and all others associated with unreachable nodes. The sender node then reinitiates route discovery if there are no other routes to the receiver node [15].

2.4.2 Dynamic Source Routing. In the DSR protocol [39], the entire route to the receiver node is supplied by the sender node and contained in the packet header. Figure 2.9 illustrates the route discovery process where the sender node S is trying to send a message to the receiver node D [39].

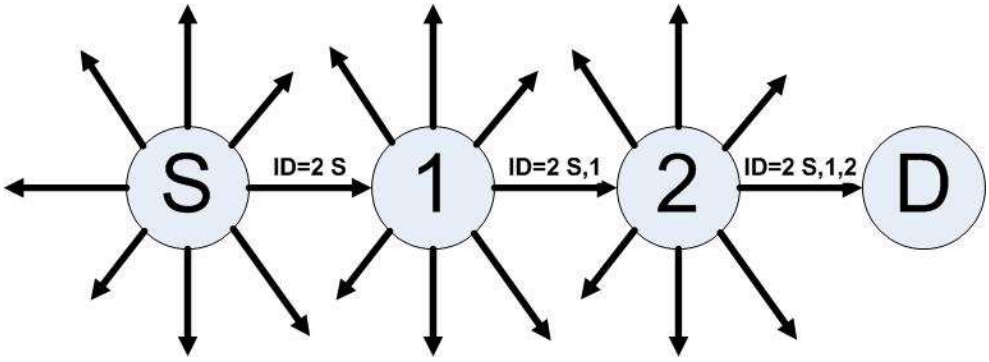

Figure 2.9: DSR Route Discovery

Sender node S begins the route discovery process by transmitting a RREQ. This packet is received by all nodes currently within the wireless range of the sender node S. Every RREQ message contains the identity of the sender, receiver, and a unique route request ID. Additionally, each RREQ message contains the intermediate nodes through which a particular copy of the RREQ message has been forwarded [39].

When another node receives an RREQ and it is the receiver node, it returns a RREP message to the sender node using either a cached route it has or by initiating its own route discovery process. If it is not the receiver node, it propagates the RREQ by transmitting it as a local broadcast packet with the same request ID.

As with AODV, each node maintains its own routing table. When a node is the sender or forwards another node's packets, it is responsible for confirming the packet has been received by the next node along the route. The receiving node sends confirmation of receipt back to the sending node. If the sending node does not receive a confirmation receipt within a specified period, a broken link is assumed, and a RERR is sent to the sender node; at this point another cached route is used, or a new route discovery process is started.

2.4.3 Multipath Routing. Ad-hoc wireless routing protocols like AODV and DSR are mainly designed to discover and use a single route between a sender and receiver node. However, multiple paths between sender and receiver nodes can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth. In Figure 2.10, the sender node has established three paths to the receiver node. If, for example, the sender node sends the same packets along all three paths and at least one of the paths does not fail, the receiver node will receive the packets.

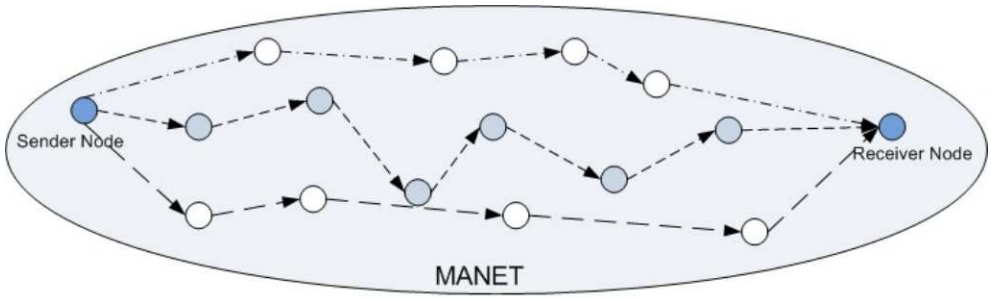

Figure 2.10: Multipath Routing

Several multipath routing protocols based on DSR have been proposed, such as Split Multipath Routing (SMR) [48], and Multipath Source Routing (MSR) [83]. Each of these multipath routing protocols broadcast data over all paths simultaneously. This technique has all the advantages previously mentioned, but it also introduces more packets into the MANET. The next section presents a technique that has the advantages of a multipath protocol without introducing extra packets into the network.

2.4.4 Round-Robin Routing. Vaidya and Lim in [82] argue that proper selection of a set of paths found by the multipath routing protocol can have a great impact on the usability of the found set of paths in terms of both delivery ratio and delay, therefore reducing not only the frequency of costly route discovery but also the overhead introduced into the network due to retry packets. Additionally, due to the dynamic topology of the network and existence of misbehaving nodes which can change their behavior over time, the best paths to take will vary. Therefore, any solution for the improvement of the availability of end-to-end communication will not be successful unless it can adapt to the state of the paths and track their behavior.

One problem addressed by multipath routing protocols is how to build multiple paths in order to maximize throughput. The key issue for the success of multipath streaming of video is to make packet loss over multiple paths as uncorrelated as possible by ensuring any one node does not affect multiple paths. Therefore, one metric for selecting multiple paths is to require them to be node-disjoint. Packet loss due to link failure or path breakage caused by nodes' movement are independent among node-disjoint paths [82].

In [28], the round-robin scheduling algorithm specifies a path is selected with the same probability among the multiple paths at the time a data packet is sent. Therefore, assuming that at time t, n paths are known at a sender s toward the receiver d. A path i is selected with probability p_i:

$$p_i = \frac{1}{n}, \quad \sum_{i=1}^{n} p_i = 1, i \in [1, 2 \ ... \ n] \tag{2.1}$$

The weighted round-robin algorithm represents a special case of the round-robin algorithm. For each path i, a weight w_i, is assigned and accordingly a path is selected with probability p_i:

$$p_i = w_i, \quad \sum_{i=1}^{n} w_i = 1, i \in [1, 2 \ ... \ n] \tag{2.2}$$

Using multiple paths in ad-hoc networks to achieve higher bandwidth is not as straightforward as in wired networks. Because ad-hoc networks communicate over a wireless medium, radio interference may be a factor when a node communicating along one path interferes with a node communicating along another path, limiting the achievable throughput [55]. Still, simulations have shown that broadcast multipath routing creates more overhead but provides better performance in congestion and capacity than unipath routing, provided the route length is within a certain upper bound which is derivable [65]. Additionally, the proper selection of routes using a round-robin multipath protocol can increase further the network throughput [28].

2.5 MANET Security Frameworks

The following sections briefly describe some of the most well-published frameworks for securing MANETs. These frameworks use either behavior grading, encryption/authentication, or IDSes to secure the network.

2.5.1 MObile Certification Authority. The framework MObile Certification Authority (MOCA) [90] employs threshold cryptography (distributing information among a cluster of cooperating computers) to distribute the Certificate Authority (CA) functionality over specially selected nodes based on the security and the physical characteristics of nodes. The selected nodes that collectively provide PKI functionality are called MOCAs.

MOCA is a key distribution framework and does not incorporate behavior grading or multipath routing. The encryption scheme employed is designed to protect data and authenticate users, but not to protect the nodes themselves.

2.5.2 Maximum Degree Algorithm. Maximum Degree Algorithm (MDA) is a fully self-organized public-key management system that allows users to generate their public/private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services [12]. This approach also does not require any trusted authority, even in the system initialization phase.

MDA is also a key distribution framework and does not incorporate behavior grading or multipath routing. Like MOCA, the encryption scheme is designed to protect data and authenticate users only.

2.5.3 Self-Organized Network-Layer Security. Self-Organized Network-Layer Security (SCAN) is a unified network layer prevention scheme that uses AODV routing [88]. It takes a self-organized approach by exploiting a full localized design without assuming any a priori trust or secret association between nodes. Each node has a token in order to participate in the network operations and its local neighbors collaboratively monitor it to detect any misbehavior in routing or packet forwarding services. Upon expiration of the token, each node renews its token via its multiple neighbors. The period of the validity of a node's token is dependent on how long it has behaved well in the network. A well-behaving node accumulates its credit and renews its token less frequently over time.

SCAN protects the network by detecting and reacting to malicious nodes. It does not employ encryption to protect the data or the nodes. It also does not address node selfishness and security threats in the network's physical and link layers. It does not use multipath routing.

2.5.4 Techniques for Intrusion Resistant Ad-hoc Routing Algorithms. Techniques for Intrusion Resistant Ad-hoc Routing Algorithms (TIARA) is a reactive scheme designed to detect and eliminate DoS attacks [68]. This framework relies on extending the capabilities of existing ad-hoc routing algorithms to handle intruders without modifying the existing routing algorithms.

TIARA protects the network through a distributed, self-configuring, wireless firewall mechanism that confines the impact of a packet flooding attack to the immediate neighborhood of the intruder node. It does not use encryption to protect the data or the nodes. It also does not use multipath routing.

2.5.5 Secure Efficient Ad-hoc Distance Vector. Secure Efficient Ad-hoc Distance Vector (SEAD) uses efficient one-way hash functions to encrypt data and does not use symmetric cryptographic operations in the protocol in order to support the nodes of limited processing capabilities [33]. The authors believe nodes in an ad-hoc network are unable to verify asymmetric signatures quick enough for routing protocols to decide on the routing path.

SEAD does not employ behavior grading mechanisms. Therefore, it is subject to numerous attacks common in MANETs. It does not use multipath routing.

2.5.6 On-demand Secure Routing Protocol. The On-demand Secure Routing Protocol (OSRP) defines a reliability metric based on past records and uses it to select a secure path in the MANET [63]. The reliability metric is represented by a list of link weights where high weights correspond to low reliability. Each node in the network maintains its own list, referred to as a weight list, and dynamically updates it when faults are detected. Faulty links are identified using a secure adaptive probing technique that is embedded in the normal packet stream.

OSRP is designed to protect the MANET from byzantine failures by detecting a malicious link after $\log n$ faults have occurred, where n is the length of the path. It

uses both encryption and behavior grading, but is not effective against many behavior based attacks nor against DoS attacks. It does not use multipath routing.

2.5.7 Alliance of Remote Instructional Authoring and Distributed Networks for Europe. Alliance of Remote Instructional Authoring and Distributed Networks for Europe (ARIADNE) prevents attackers from tampering with uncompromised routes consisting of uncompromised nodes [34]. It is based on the DSR protocol and relies on symmetric cryptography only. It operates in three stages. The first stage presents a mechanism that enables the target to verify the authenticity of the route request. The second stage presents a key management protocol that relies on synchronized clocks, digital signatures, and standard message authentication code for authenticating data in route requests and route replies. The third stage presents an efficient per-hop hashing technique to verify that no node is missing from the node list in the route request.

ARIADNE uses encryption to authenticate nodes and protect data, but it is not used to protect nodes from direct attacks. DoS attacks are not addressed. It uses a behavior grading mechanism similar to RIPSec's, taking advantage of DSR's error messages. It does not use multipath routing.

2.5.8 Security Aware Ad-hoc Routing. The Security Aware ad-hoc Routing protocol (SAR) is based on on-demand protocols, such as AODV and DSR [91]. In SAR, a security metric is added into the route request packet and a different route discovery procedure is used. Relay nodes receive a route request packet with a particular security metric or trust level. At the relay node, if the security metric or trust level is satisfied, the node will process the route request packet and propagate it to its neighbors using controlled flooding. Otherwise, the route request is dropped. If an end-to-end path with the required security attributes can be found, the receiver will generate a route reply packet with the specific security metric. If the receiver node fails to find a route with the required security metric or trust level, it sends a

notification to the sender and allows the sender to adjust the security level in order to find a route.

SAR uses encryption to protect data but does not protect individual nodes from attack. Behavior grading is not used to protect the MANET against common attacks.

2.5.9 Collaborative Reputation Mechanism. The Collaborative Reputation Mechanism to Enforce Node Cooperation (CORE) is a framework based on reputation to enforce cooperation among MANET nodes to prevent selfish behavior [54]. Each network node keeps track of other nodes' collaboration using their reputation. The reputation is calculated based on various types of information on each node's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented. Three types of reputation are used: subjective, indirect, and functional.

CORE does not use encryption for the protection of data or nodes. It does use behavior grading based on nodes' ability to participate in the routing process and the ability to relay packets, but it is susceptible to many well-known MANET attacks.

2.5.10 Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks. The Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks (CONFIDANT) protocol attempts to make node misbehavior unattractive by detecting and isolating offending nodes [11]. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. It is built on the DSR protocol.

CONFIDANT uses encryption only to authenticate messages. It does not protect the data or individual nodes. It uses behavior grading to ensure nodes participate in the routing process and forward packets. However, it is vulnerable to many MANET attacks. It does not use multipath routing.

2.5.11 Watchdog and Pathrater. Watchdog and Pathrater are designed to work with the DSR protocol [84], both operating at the node level of a MANET. The Watchdog detects misbehaving nodes while the Pathrater chooses the most secure route to take when sending packets. The Watchdog measures a neighboring node's frequency of dropping or misrouting packets, or its frequency of invalid routing information advertisements. Watchdog maintains a buffer of recently sent packets and compares each overheard packet with the packets in the buffer to see if there is a match. If there is a match, the node removes the packet from the buffer. If a packet has remained in the buffer too long, the Watchdog increments a failure tally for the neighboring node. If the tally exceeds a certain threshold, it sends a message to the sender node notifying it of the misbehaving node. The weaknesses of Watchdog are that it might not detect a misbehaving node because of ambiguous collisions, receiver collisions, limited transmission power, false behavior, collusion, and partial dropping. A node might be accused of being malicious for the same reasons. Pathrater keeps track of the trustworthiness rating of every known node. It calculates path metrics by averaging the node ratings in the path to each known node. If there are multiple paths to the same receiver, then the path with the highest metric is chosen.

Watchdog and Pathrater do not use encryption to protect data or nodes. They do use behavior grading by monitoring downstream nodes, but are vulnerable to numerous MANET behavior attacks. They do not use multipath routing.

2.6 Trust Management in Ad-hoc Networks

Section 2.5 presented limited security solutions. This section introduces some broader frameworks that address trust management and key distribution in frameworks protected by encryption and behavior grading.

Hadjichristofi presents a representative Key Management System (KMS) in [31]. The KMS manages user identity certificates and establishes rules for issuing, reissuing, and revoking certificates. In a decentralized environment like a MANET, the goal is to provide the KMS with access control decisions based on the trustworthiness

of the perspective peer node. Likewise, Adams [1] presents a representative Trust Management System (TMS) architecture in Figure 2.11 that implements a central, data processing layer of the overall system security architecture. The KMS and IDS are depicted at the top and bottom of the diagram, respectively. Arrows show how the modules exchange information from these two entities. The center of the diagram shows how a node processes, evaluates, and stores the behavior information using the trust store and the reputation scaling module. The risk assessment module continually adjusts trust thresholds based on current network conditions. When the KMS requests a trust decision, the prospective node's reputation is compared to the current trust threshold. Once the evaluation is complete, the TMS forwards an access control decision to the KMS.

The TMS provides the KMS with a layer of abstraction of the overall trustworthiness of nodes, based on the activity of the nodes in the network. The TMS resides on each node and helps to determine whether to trust or distrust its peers based on its individual trust thresholds. The TMS reports its trust decisions to the KMS for its consideration. The input to the TMS is an IDS or a monitoring scheme. MANET IDSes can detect many types of attack, but are too easily tricked, fooled, and bypassed to be reliable security devices, though they can be of some benefit [58]. Therefore, a monitoring system based on behavior (such as CORE [54]) is more appropriate.

To quantify trust, the TMS generates a Reputation Index (RI) on each and every node. When one of the MANET nodes reports an observation of another node, the reporting node's RI is used as a factor in creating a Feedback Item (FI). The following formula demonstrates how an FI may be calculated. $FI = RI_x \times obs_x$ where RI_x is the reporting node x's reputation and obs_x is a periodic observation by node x [1]. The calculation method aggregates FIs in an exponential weighted moving average. FIs are used to generate the overall RI. In Adams' framework, RIs have a value between -1 and 1, where -1 means the node is not trusted at all, and +1 means the node is completely trusted. An RI value of zero means the node's reputation is neutral. As stated previously, the RI is used as input to the KMS to determine

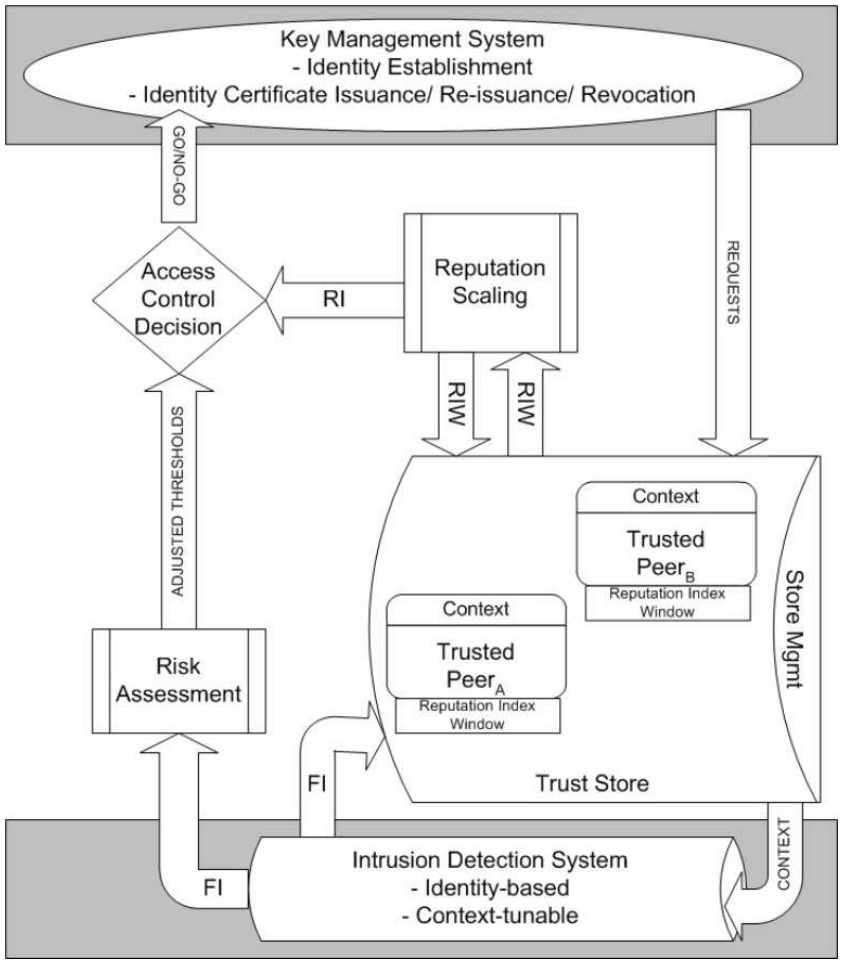

Figure 2.11: Trust Management System Architecture [1]

whether or not certificates should be renewed or revoked. The following excerpts summarize Adams' trust model [1].

- Trust is context dependent
- Trust has positive and negative degrees of trustworthiness
- Trust is expressed in continuous values
- Trust is based on experiences and observations between individuals
- Trust information is exchanged between nodes
- Trust is subjective. Nodes calculate different reputation values for the same observed node
- Trust is dynamic and is modified, in a positive or negative direction, based on new observations and reports

2.7 Tying It All Together

A MANET is a collection of mobile routers that move dynamically in unpredictable directions. The links connecting the nodes are wireless and thus are not as dependable as wired links. The links are also susceptible to capacity constraints. A MANET environment is characterized by numerous security threats because the wireless links are vulnerable and the nodes have little physical protection. To counteract these threats, a MANET must provide authentication, confidentiality, nonrepudiation, and increase the network services availability. Cryptography can provide these services by utilizing different cryptographic functions in a variety of combinations. IPSec is selected for this research because it is implemented at the network level and provides many advantages to protecting both data and nodes.

The setup of trust among nodes is achieved through mutual authentication techniques (PKI certificates). Two nodes authenticate with one another by presenting a valid PKI certificate that is negotiated with out-of-band methods to prevent attacks on the key distribution mechanism.

A critical component of the security framework is the monitoring of node behavior. Reputation Indexes (RIs) assigned to nodes based on observed and reported behavior determine whether or not a node is allowed to participate in a route between sender and receiver nodes.

Round-robin multipath routing increases network availability by using only routes that have a high probability of reaching the receiver node, enabling mission-critical multimedia applications to operate in the MANET.

Existing MANET security frameworks were presented to demonstrate the various methodologies' strengths and weaknesses. Additionally, key and trust management systems were presented as examples of partially integrated security solutions for MANETs. None of these solutions address all security requirements, which is why this research is needed.

This research presents a hybrid security solution for MANETs operating in a hostile environment entitled Reputation-based Internet Protocol Security (RIPSec) that addresses the shortcomings of other MANET security frameworks. As is often the case, the protocols used by a MANET are designed to provide functionality and not necessarily security. RIPSec extends Adams' [1] use of reputation indexes and feedback items into a framework that integrates functionality and security in MANETs by providing confidentiality and integrity through an implementation of IPSec in transport mode, availability through round-robin multipath routing/behavior grading, trust through a reputation management system, and authentication/non repudiation through PKI certificates. Chapter 3 presents the system design and the proposed approach to solve the research problem.

3. RIPSec Design

3.1 Chapter Overview

As stated in Chapter 1, the goals of this research are to provide a MANET that will function with multiple levels of security in a hostile environment without degrading network performance. Required security services include authentication, confidentiality, integrity, availability, and non-repudiation and will be incorporated into RIPSec in the following manner:

- Authentication will be provided by PKI certificates
- Confidentiality will be provided by PKI certificates and IPSec transport mode
- Integrity will be provided by PKI certificates and IPSec transport mode
- Availability will be provided by behavior grading and round-robin multipath routing
- Non-repudiation will be provided by PKI certificates and IPSec transport mode

This chapter presents the design and development for Reputation-based IPSec (RIPSec), a framework developed through this research for integrating network load balancing with Internet Protocol Security (IPSec) and behavior grading in a Mobile Ad-Hoc Network (MANET) environment using a modified version of the Dynamic Source Routing (DSR) protocol. As discussed in Chapter 2, a hybrid approach is required.

This chapter begins with the motivation for RIPSec in Section 3.2. Section 3.3.1 defines the roles of MANET nodes in this framework. Section 3.3.2 formalizes the relationships between nodes and paths. Section 3.3.3 explains how nodes interact securely with PKI certificates and IPSec. Section 3.3.4 describes RIPSec's behavior grading mechanism while Section 3.3.5 details the routing process. A summary of the chapter is presented in Section 3.4.

3.2 Design

RIPSec is designed to operate in a closed MANET, meaning only authorized nodes can join and leave the network. All nodes in the MANET are known and trusted initially. Figure 3.1 shows the major components of a RIPSec-enabled MANET and is described below.

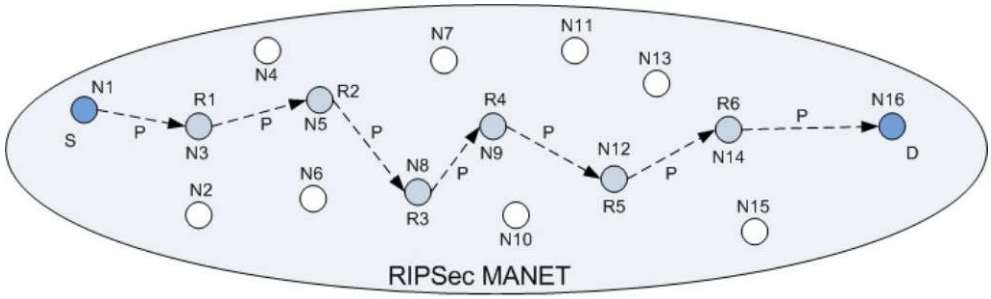

Figure 3.1: RIPSec MANET Components

3.2.1 Node Roles. Nodes may perform multiple roles simultaneously. In this framework, the following roles are defined:

- Sender Node - A node originating data to be sent to a receiver node
- Receiver Node - Also known as a sink, this node is the receiver and final destination of data from a sender node
- Relay Node - Also known as a router, this node serves as a conduit between a sender and receiver node pair that cannot communicate directly with each other

3.2.2 Node Formalization. RIPSec nodes form paths between sender and receiver nodes using relay nodes. The following is a formalization of the node/path relationships.

- $N =$ a set of MANET nodes $\{N_1, N_2, ..., N_M\}$
- $M =$ the number of nodes in the MANET

- $S =$ a sender node
- $D =$ a receiver node
- $R =$ a set of relay nodes $\{R_1, R_2, ..., R_k\}$ where there are $k+1$ hops between S and D
- $P =$ a path consisting of $\{S, R_1, R_2, ..., R_k, D\}$ where the elements of P are all distinct members of set N

In Figure 3.1, a path P exists from sender node S to receiver node D, where $S = N_1$ and $D = N_{16}$. There are $k = 6$ relay nodes (7 hops total) between node S and node D. Relay node $R_1 = N_3$, node $R_2 = N_5$, ..., node $R_6 = N_{14}$. The complete path is annotated as $P = \{N_1, N_3, N_5, N_8, N_9, N_{12}, N_{14}, N_{16}\}$.

Because there are normally multiple communication paths at one time in a MANET, the notation can be generalized as follows:

- $P_m = \{S_m, R_{1_m}, R_{2_m}, ..., R_{k_m}, D_m\}$
- $P_n = \{S_n, R_{1_n}, R_{2_n}, ..., R_{k_n}, D_n\}$

where m and n are path numbers and $m \neq n$. Additionally, k_m and k_n are the number of relay nodes in the mth and nth paths, respectively.

A node N_j can be part of one or more paths. For example, in Figure 3.2, $N_9 = R_{4_1} = R_{2_2}$. Likewise, a node might not be part of any path (e.g., N_4, N_7).

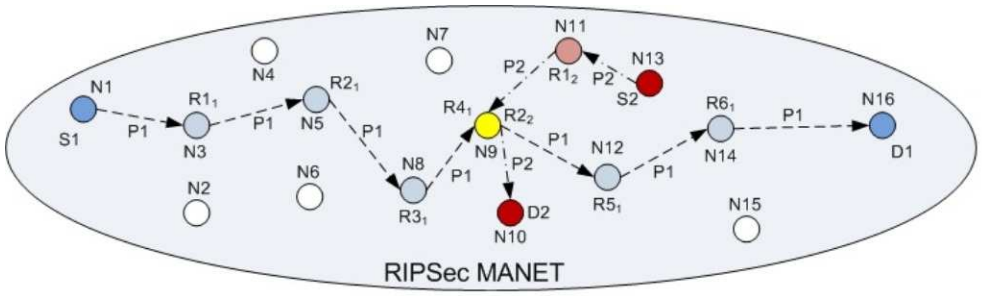

Figure 3.2: Multiple Paths in a RIPSec MANET

The two paths shown in Figure 3.2 are defined as $P_1 = \{N_1, N_3, N_5, N_8, N_9, N_{12}, N_{14}, N_{16}\}$ and $P_2 = \{N_{13}, N_{11}, N_9, N_{10}\}$. One node, N_9, is part of both paths: $R_{2_2} = R_{4_1} = N_9$.

3.2.3 Confidentiality and Integrity. Before RIPSec nodes are deployed, PKI certificates are distributed out-of-band to all nodes N_j so that each node has its own public/private certificate pair and the public certificate for each node participating in the closed MANET. The only known attacks against IPSec are against the Internet Key Exchange (IKE) protocol [73]. Distributing the certificates securely through means other than IKE eliminates this particular attack. The PKI certificates are used to sign and encrypt data and to establish IPSec Security Associations (SAs).

SAs must be established for communication to occur between nodes N_l and N_m. Every node pair has two pairs of SAs detailing the bidirectional connections between them. One pair is for authentication, and the second pair is for encrypting data. Each pair of SAs consists of an inbound rule and an outbound rule for a given node. Both rules must exist for nodes to communicate with each other. A formalization of RIPSec SAs is provided next, in conjunction with Figure 3.3.

- Let N_l and N_m be two nodes forming an SA relationship
- SA_{l_m} is a set of SAs, $SA_{l_m} = \{SA_{l_{mai}}, SA_{l_{mao}}, SA_{l_{mei}}, SA_{l_{meo}}\}$ associated with nodes N_l and N_m where a is the SA for authentication, e is the SA for encryption, i is the inbound rule from node N_m to node N_l and o is the outbound rule from node N_l to node N_m. This set of SAs exists only on node N_l. A complementary set of SAs, SA_{m_l}, must exist on node N_m before communication can take place.
- SA_{m_l} is a set of SAs, $SA_{m_l} = \{SA_{m_{lai}}, SA_{m_{lao}}, SA_{m_{lei}}, SA_{m_{leo}}\}$ associated with nodes N_m and N_l where a is the SA for authentication, e is the SA for encryption, i is the inbound rule from node N_l to node N_m and o is the outbound rule from node N_m to node N_l. This set of SAs exists only on node N_m.

Packets are sent to the next hop in the route via IPSec encrypted links to protect the data from disclosure. IPSec helps protect the nodes themselves from external threats by refusing any connections that do not match the node's security policy. In RIPSec, IPSec is deployed in transport mode. This mode behaves like a firewall and is very effective at preventing unauthorized access to a member node.

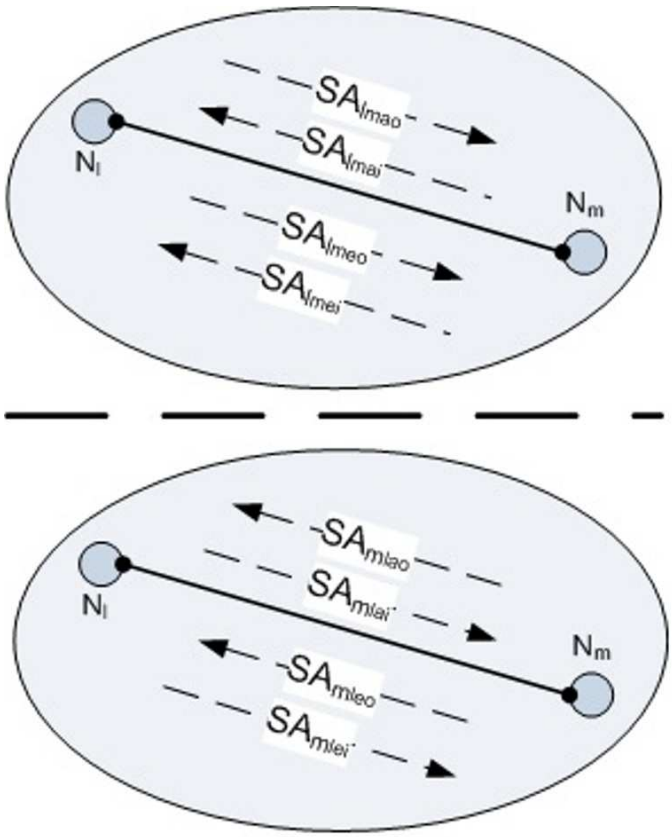

Figure 3.3: Security Associations Between Nodes

However, before data can be sent to a receiver node, it must be safeguarded from disclosure, illustrated in Figure 3.4.

When the sender node S_1 is prepared to send data, it will first encrypt the data with the receiver node D_1's public certificate, protecting the data from disclosure. A digital signature is created by computing a digest of the encrypted data with Secure Hash Algorithm 1 (SHA-1). In [51], a comparison between SHA-1 and Message Digest 5 (MD5) indicates SHA-1 is much more effective against brute force attacks than is MD5. SHA-1's digest is 32 bits longer than the MD5 digest. Using a brute force technique, the difficulty of producing any message having a given message digest is on the order of 2^{128} operations for MD5 and 2^{160} operations for SHA-1. The difficulty of producing two messages with the same message digest is on the order of 2^{64} operations for MD5 and 2^{80} for SHA-1. Therefore, SHA-1 is considerably stronger against brute

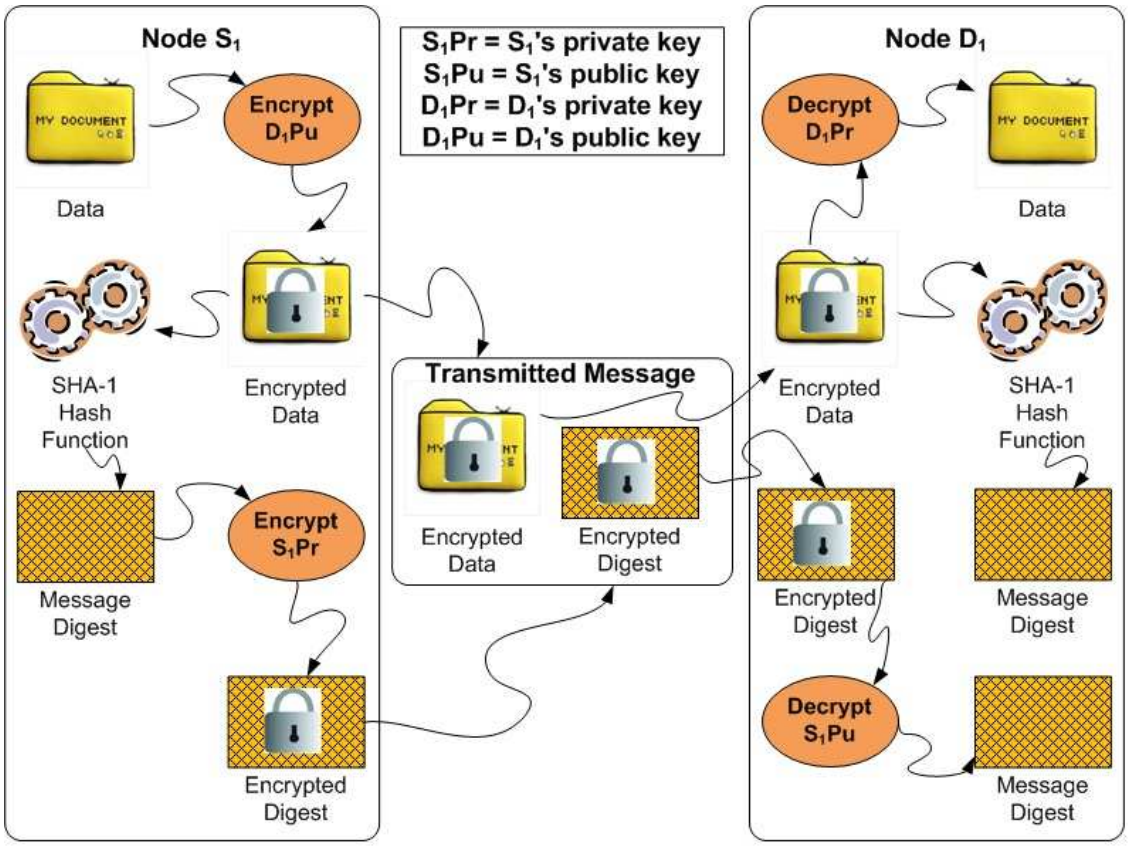

Figure 3.4: Transmitting Data

force attacks than is MD5. MD5 is vulnerable to cryptanalytic attacks discovered since its design [76]. SHA-1 appears not to be vulnerable to such attacks. Both algorithms perform well on 32 bit architectures because they rely heavily on addition modulo 2^{32}. SHA-1 involves more steps (80 versus 64) and must process a 160-bit buffer compared to MD5's 128-bit buffer. Therefore, SHA-1 should execute more slowly than MD5 on the same hardware. Although slower to compute, SHA-1 is the digest choice for RIPSec because it is much more secure.

The digest is encrypted with the sender node S_1's private certificate and both the encrypted message and encrypted digest are sent to the receiver node, D_1. The receiver node D_1 computes a digest of the received message using the sender node S_1's public certificate. The receiver node D_1 also decrypts the encrypted digest using the sender node S_1's public certificate and compares the two digests. If they are equal,

the message is verified to be from the sender node S_1 and is then decrypted using the receiver node D_1 private certificate. The data can now be read and is assured to be authentic and correct.

A relay node is acting as a router and should have no concern what the data is and will not be able to read it. Its only job is to forward the data to the next hop in the route. In RIPSec, a relay node can verify the sender of data but cannot read it because it does not have the correct certificate for decryption. Only the receiver node has the appropriate certificate that will decrypt the data. The use of PKI certificates protects the data from any compromised nodes that are still participating in the transfer of data.

3.2.4 Reputation and Behavior Grading. Sender and relay nodes monitor downstream nodes to confirm if packets are received and acknowledged. Upstream nodes (sender or relay) will increment the RI in their RI table for downstream relay nodes that acknowledge receipt of packets. Receiver nodes are not graded because they cannot be excluded from the sender route as there would be no alternative receiver node. Conversely, the RI entries are decremented when upstream nodes do not receive an acknowledgment from a downstream node within 0.5 seconds (default setting for DSR). If a sender node does not receive an acknowledgment at all, the route is considered broken and deleted from the route cache.

The limits of the calculated RI are machine dependent and were $\pm 2,147,483,647$ in the OPNET simulations on a 64-bit computer. Typical RI values ranged between ± 500. The formula for calculating a node's RI is given as

$$RI_{ij\ new} = RI_{ij\ old} + FI_{ijk} \text{ where } FI_{ijk} = \pm 1 \tag{3.1}$$

where RI_{ij} = Reputation Index, FI_{ijk} = Feedback Item, i = the node forming the opinion, j = the node the opinion is being formed on and k = the node providing feedback on node j.

The RIs are then used in the next route discovery process to determine if a node can be part of a route from sender to receiver. Additionally, when a node's RI becomes negative, the perceiving node searches through its route cache and all routes using that node are deleted. This process is implemented in RIPSec and in the simulations.

RIPSec's behavior grading mechanism does not prevent a node from hoarding packets. A misbehaving node displaying malicious behavior could acknowledge receipt of packets but not forward them to the next hop. This action could only result in a minor disruption of service, given the data cannot be read except by the intended receiver node. The malicious node is responsible for generating a route error if it cannot deliver the packet to the next downstream node, but since it is intentionally hoarding packets, it will not generate an error and the upstream node will keep sending it packets. In this scenario, the receiver node will continue to receive packets delivered through other routes utilized by the sender node, assuming other routes exist, preventing a complete disruption of service. If necessary, higher layers of the protocol stack, such as TCP, could repeat the data transmission.

Once a sender node sends data to a relay node, it waits for an acknowledgment that the data was received (0.5 seconds, customizable in the DSR parameters). If it receives an acknowledgment, it increments its perception of the cooperating relay node's RI. If the sending node does not receive an acknowledgment from the relay node, it retransmits another acknowledgment request. After the acknowledgment request has been retransmitted the maximum number of times (2 in this framework, customizable in the DSR parameters), and no response is received (ACK or error), the sender node treats the link as broken and reports a route error to each node that has sent a packet routed over that path since the last acknowledgment was received. Error conditions may be caused by misbehaving or non-misbehaving nodes. The node originating the route error and all nodes receiving the route error update their RI table by decrementing the offending relay nodes' RI by 1 to reflect the error condition.

When sending or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that data can flow over the link from that node to the next hop. For example, in Figure 3.5 node S_1 sends data through nodes R_{1_1}, R_{2_1}, R_{3_1}, R_{4_1}, R_{5_1}, and R_{6_1} respectively to the receiver node D_1. Node S_1 is responsible for the link from node S_1 to node R_{1_1}. Node R_{1_1} is responsible for the link from node R_{1_1} to node R_{2_1}, and so on. An acknowledgment provides confirmation that a link is capable of carrying data, and in wireless networks, acknowledgments are often provided as an existing standard part of the MAC protocol in use, such as IEEE 802.11, or by a "passive acknowledgment" in which, for example, node R_{1_1} confirms receipt at node R_{2_1} by overhearing node R_{2_1} transmit the packet when forwarding it on to node R_{3_1}. In addition to the built-in acknowledgment mechanism, the node transmitting the packet explicitly requests that a DSR-specific software acknowledgment be returned by the next node along the route. If an acknowledgment is received by the transmitting node, that constitutes a positive feedback item and increases the reputation index of the acknowledging node by 1. However, after the acknowledgment request has been retransmitted the implementation specific maximum number of times and no acknowledgment has been received, then the sender treats the link to this next-hop destination as currently "broken". Per DSR protocol rules, the link will be removed from the sending node's route cache and a "route error" transmitted to each node that has sent a packet routed over that link since an acknowledgment was last received. For example, in the situation above, if node R_{2_1} does not receive an acknowledgment from node R_{3_1} after some number of requests, it will return a route error to node S_1 (negative feedback item), as well as any other node that may have used the link from node R_{2_1} to node R_{3_1} since node R_{2_1} last received an acknowledgment from node R_{3_1}. Since node R_{2_1} detected the error, it has first-hand knowledge that node R_{3_1} caused an error (negative feedback item) and thus decrements node R_{3_1}'s reputation index from its point of view. Node S_1 has second-hand knowledge that node R_{3_1} caused an error and decrements node R_{3_1}'s reputation index by one from its point of view.

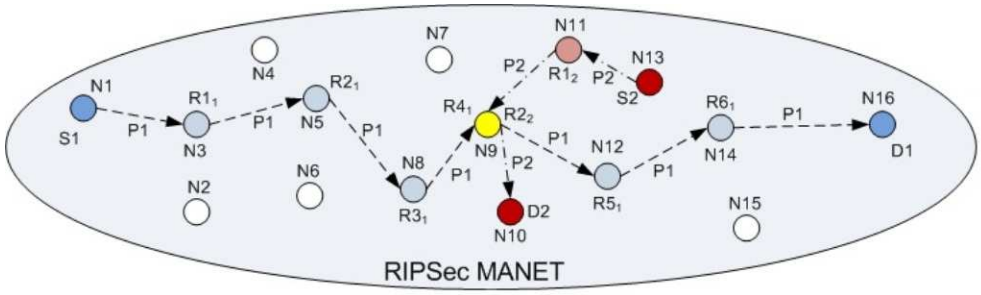

Figure 3.5: RIPSec Feedback Items

Every node calculates and maintains its own perception of every member node's RI in an RI index table. Any node that has a negative RI will be considered untrusted and will not be included when generating a route to a receiver. Conversely, a node with a non-negative RI is trusted and will be considered in the routing process. Even though a sender node will not use a node with a negative reputation when determining a route to a receiver, a node with a negative reputation may remain part of a route for a different sender node because it may still have a good reputation perceived by that particular sender node. This is illustrated in Figure 3.6 where path $P_1 = \{S_1, R_{1_1}, R_{2_1}, R_{3_1}, R_{4_1}, R_{5_1}, D_1\}$ and path $P_2 = \{S_2, R_{1_2}, D_2\}$

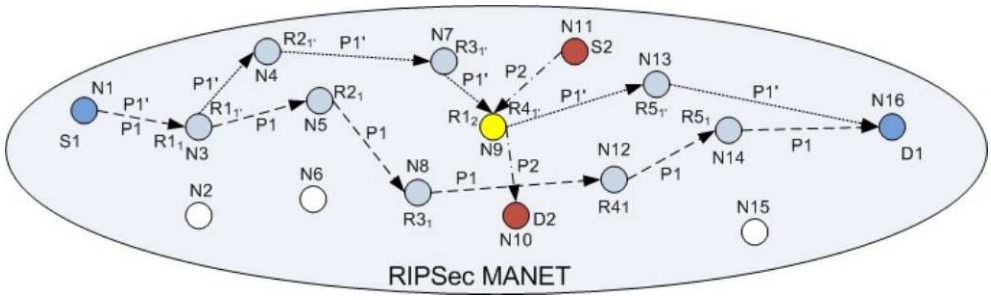

Figure 3.6: Negative Reputation Node Participation

A route from sender node S_1 to receiver node D_1 can have several candidate paths (P_1 and $P_{1'}$), and based on its internal RI table, S_1 decides not to use certain paths because a node does not have a good RI. However, that same node (i.e., N_9) could still be seen favorably by other sender nodes (i.e., S_2). In Figure 3.6, path $P_{1'}$ is rejected by node S_1 because node N_9 has a negative RI.

Even though node S_1 will not use node N_9 when forming its own route to a receiver, it still communicates with it as a relay node and perhaps as part of another source node's route to a receiver node D. This mechanism allows a node with a negative reputation, as is the case with node N_9 from the perspective of node S_1, to regain a positive reputation by relaying packets from node S_1. Every acknowledged packet by node N_9 to S_1 (which is also N_1) earns positive feedback that influences node N_1's perception of node N_9's reputation, annotated as RI_{1_9}. If a node never communicates with another node it perceives to have a negative reputation, there is no way for the ostracized node to regain a positive reputation.

3.2.4.1 Feedback Nodes. One strategy for determining the appropriate time to decrement a node's RI is to wait until more than one node provides negative feedback on a particular node. Allowing some number of nodes, more than one, to corroborate a particular node's error condition gives the offending node a certain amount of leeway before taking action against it. However, optimization of throughput is a primary goal of this framework and the deciding factor when determining how many nodes should provide negative feedback before decrementing the RI.

The number of nodes providing feedback on a particular node ranges from 0 (the node is not part of any paths) to $M-1$, with M total nodes in the MANET. Table 3.1 illustrates the impact on *route errors sent*, *load*, and *throughput* when varying the number of nodes providing negative feedback before decrementing a node's RI. A mildly stressed MANET, defined as 50 nodes with 25 of the nodes misbehaving 50% of the time, was used to determine the optimum number of feedback nodes. Misbehavior was simulated by destroying the designated percentage, in this instance 50%, of the packets received by a misbehaving node. According to simulation results, only one feedback node is required to provide the highest throughput. If more than one feedback node is used before decrementing a node's reputation, the model is too slow to respond to the error-prone node. The other two metrics, Avg Route Errors and Avg Load with one feedback node, are either worse or at least comparable to the

results obtained with more than one feedback node and thus are acceptable. Tables B.3, B.4, B.5, B.6, B.7, B.8 in Appendix B contain the actual data used to determine the appropiate number of feedback nodes.

Table 3.1: Feedback Nodes Metrics

Fdbk Nodes	**Avg Route Errors**	**Avg Load**	**Avg Throughput**
1	414.7601	14,103,611.6579	4,079,123.0517
2	393.1740	13,677,721.7726	2,670,669.5588
3	404.5274	13,620,072.2690	2,577,642.5801
4	407.6352	13,280,350.0801	3,313,072.0754
5	467.4740	13,555,381.1868	2,800,073.9260
6	493.0750	13,542,138.7350	3,265,766.3106

3.2.5 Routing. When a sender node needs to send data to a receiver node, it must first acquire a route to the receiver node. In the RIPSec route discovery process, nodes with a negative reputation are eliminated from participating in the route.

RIPSec uses a modified version of the DSR protocol for routing. The sender node broadcasts to all neighbor nodes that a route is needed to the receiver node. RIPSec will limit the broadcast only to nodes that do not have a negative RI. The restriction is implemented by removing all nodes with a negative RI from the array of neighbor nodes maintained by DSR. If any of the remaining neighbor nodes have a route to the receiver node advertised, the node(s) will reply back to the sender node with the route. If they do not have a route, they forward the route request to their neighbor nodes until eventually the receiver node is reached and replys with a route from the sender to the receiver. In cases where there is no route from sender to receiver, the sender node continues to broadcast a route request until a route is available or until the process times out. It is also possible that multiple routes will be discovered. Typically, the sender node will use only the first route it discovers, which in most cases will also be the shortest route. However, RIPSec makes use of all discovered routes in a round-robin fashion to distribute the network load in the MANET.

In RIPSec, the following sequence determines the routes used to send data from sender node S_1 to receiver node D_1.

- Sender node S_1 requests a route to receiver node D_1
- All possible routes are discovered by the DSR protocol and stored in sender node S_1's route cache
- The routes containing negative reputation nodes are removed from sender node S_1's route cache
- The remaining routes are used in round-robin fashion to send the data to receiver node D_1

This provides the best opportunity for data to get from sender to receiver by avoiding problematic nodes/paths.

All discovered routes are cached at each node by default. To utilize multiple routes, the first packet to be sent utilizes the first route in the cache, which is normally the only route used by DSR. In RIPSec, the second packet to be sent utilizes the second route in the cache, and the third packet the third route. This pattern continues until all routes in the cache are used. The next packet to be sent then rotates back to the first route in the cache and the process repeats itself until all packets have been sent.

The route cache is continuously updated by the DSR route discovery process. It is entirely possible that the set of routes in the cache changes between the start and completion of data transmission, especially given the mobile nature of a MANET's nodes. This has no adverse effect on RIPSec, as the routes used are pulled from the route cache in a round-robin fashion.

3.3 Summary

This chapter presented the design for RIPSec, a framework developed through this research for integrating network load balancing with Internet Protocol Security (IPSec) and behavior grading in a Mobile Ad-Hoc Network (MANET) environment.

The motivation for RIPSec was provided along with the design and development of the framework.

Chapter 4 presents the simulation methodology for assessing the performance of RIPSec.

4. Simulation Methodology

4.1 Chapter Overview

This chapter presents the methodology for assessing the performance of RIPSec. The following section details the simulation environment and architecture models. Section 4.3 describes the simulation equipment used. Sections 4.4 and 4.5 describe the model's performance metrics and validation respectively. The chapter concludes with a summary in Section 4.6.

4.2 Simulation Environment and Architecture Models

The previous chapter described RIPSec and its design for operation. It was not feasible to implement an empirical experiment of RIPSec with actual resources. Instead, RIPSec was implemented with simulation using OPNET simulation software.

4.2.1 Simulation Environment. The OPNET simulator was chosen over Network Simulator 2 (NS2) and GloMoSim due to the availability of both local and vendor support. The visualization capabilities of OPNET were also an advantage over the other simulators. The following sections describe the simulation parameters.

4.2.1.1 System Under Test. The system under test is RIPSec and its three core components: IPSec encrypted links between nodes, behavior grading of nodes, and round-robin multipath routing to distribute the network load of video conferencing applications.

4.2.1.2 System Services and Outcomes. The system services and outcomes for the core components of RIPSec are as follows:

- IPSec encryption - Security Associations between nodes, simulated by increasing all packet sizes 36 bytes to account for the overhead induced size increase of IPSec wrapped packets [4].

- Behavior grading - Feedback generated by observation of downstream node behavior and Reputation Indexes calculated from the feedback.
- Load distribution - Multiple routes, all used by the DSR protocol, to distribute the network load of video conferencing applications and reduce the dependence on any one node in the closed MANET.

4.2.1.3 System Parameters. The system parameters in Table 4.1 were used in the RIPSec simulation environment. These parameters were either stated explicitly in [10], selection based on similarity to the proposed framework, or were inferred based on the research of published data in [47].

Table 4.1: OPNET Simulation Parameters

Parameter	**Value**
MAC Protocol	802.11b
Max Throughput	11 Mbps
Movement Model	Default Random Waypoint
Ad-Hoc Routing Protocol	DSR
Nodes in Simulation	50
Sender Nodes	1 (Node 9)
Receiver Nodes	1 (Node 1)
Transmission Range	250 meters
Transmit Power	0.0002 watts
Simulation Area	670 meters x 670 meters
Simulation Time	2700 seconds
Node Speed	Uniform 0 - 10 meters/second
Mobility Pause Time	Constant 100 seconds
Mobility Start Time	Constant 10 seconds
Mobility Stop Time	End of Simulation
Mobility Max x and y	500 meters
Packet Size w/o RIPSec	64 bytes
Packet Size w RIPSec	96 bytes
Number of simulations per scenario	4 (see C.O.V)
Simulation Seeds	25, 132, 145, 150
Video Conferencing	High Resolution Video
	128 x 240 pixels
	9 bits/pixel
	15 frames/second

4.2.2 Coefficient of Variation. The Coefficient of Variation (C.O.V.) [36] is the ratio of the sample standard deviation to the sample mean.

$$C.O.V. = \frac{s}{\overline{x}} \tag{4.1}$$

A C.O.V. of less than 10% is generally used as the stopping criteria for simulations. The C.O.V. for errors sent, load, and throughput was calculated during each run of the simulations and results collected for analysis in Appendix C indicated four repetitions were sufficient to achieve non-overlapping interval bounds for the scenarios at 90% confidence.

4.2.2.1 Factors. The factors selected for use in this study are shown in Table 4.2. Treatment levels were chosen based on guidance from [69]. The factor levels are varied to observe the effect on performance of the RIPSec enabled closed MANET. These factors were chosen to determine the results of a mildly, moderately, and heavily stressed MANET. Moderately stressed is defined as 50% of the nodes (25 of 50) operating at 50% misbehavior. Mildly stressed is defined as 10 of 50 nodes operating at 10% misbehavior, and heavily stressed is defined as 40 of 50 nodes operating at 50% misbehavior. The MANET was functional at the highest treatment level (40 nodes/50 % misbehavior). A misbehavior level of 75% was attempted during preliminary simulations, but the MANET could not sustain operations with 40 of the 50 nodes misbehaving 75% of the time. Therefore, after consulting with faculty, 40 nodes operating at 50% misbehavior was determined to be sufficient treatment to heavily stress the network.

Table 4.2: RIPSec Factors and Levels

Factor	**Level**
Num of Misbehaving Nodes	10, 25, 40
Percentage of Misbehavior	10, 50
RIPSec Enabled	On, Off

4.2.3 Experimental Design. The experimental design is a balanced, full factorial model with replications. This design allows studying the effect of each factor level, as well as the effects of any interactions between factors on the response variable. Each factor combination is replicated four times, based on C.O.V. results, with different seeds. The replication allows the computation of error for statistical analysis. Table 4.3 provides all the factor level combinations. The total number of runs needed for this experiment is 48 and computed as follows:

$$3\ Levels^{1\ Factor} \times 2\ Levels^{2\ Factors} \times 4\ Replications = N \tag{4.2}$$

$$3^1 \times 2^2 \times 4 = 48 \tag{4.3}$$

Table 4.3: RIPSec Factor Level Combinations

Num Misbehaving Nodes	**Percent Misbehavior**	**RIPSec**
10	10	off
10	10	on
10	50	off
10	50	on
25	10	off
25	10	on
25	50	off
25	50	on
40	10	off
40	10	on
40	50	off
40	50	on

4.2.4 Confidence Interval. The confidence level for this research is 90%, chosen due to the variance in means of simulation runs. When the simulated MANET was mildly or moderately stressed, the simulation means were very similar. However, when the MANET was heavily stressed, simulation means were more varied.

When an experiment has a 90% confidence level with an interval of plus or minus 10%, there is a 90% probability that the actual mean value of the experiment lies within a range 10% above and 10% below the experimental mean [36]. The confidence interval is given by

$$\left(\overline{x} - z_{1-(\frac{\alpha}{2})}\left(\frac{s}{\sqrt{n}}\right), \overline{x} + z_{1-(\frac{\alpha}{2})}\left(\frac{s}{\sqrt{n}}\right)\right) \tag{4.4}$$

where $\overline{x}$ is the sample mean, $z_{1-(\frac{\alpha}{2})}$ is the $1-(\frac{\alpha}{2})$ quantile of a unit normal variate (1.645 for 90% confidence if more than 30 samples are used), s is the standard deviation, and n is the number of samples. If the means of two experiments fall within the confidence intervals of each other, then the two items being compared are statistically identical. If the confidence interval does not contain the mean, then the items being compared may be statistically different at this confidence level and a t-test would need to be performed to confirm the difference.

4.2.5 Analysis of Variance. In this research, three factors are used: number of misbehaving nodes, percentage of misbehavior, and RIPSec on/off. This is called a factorial design and requires experimental runs be made at all possible combinations of the factor levels. An Analysis of Variance (ANOVA) gives a statistical test to determine whether the means of more than two groups are all equal, generalizing the 2-sample t-test to more than two groups.

ANOVA decompositions for factorial designs contain a sum of squares term for every possible main effect and interaction. For example, a factorial design based on factors A, B, and C gives rise to three main effects terms (A, B, and C), three 2-factor interactions (AB, AC, and BC), and one 3-factor interaction (ABC). The sum of squares for an interaction term is denoted by putting the interaction term in parentheses after the SS notation. Thus, SS(AB) denotes the sum of squares associated with the AB interaction, SS(ABC) is the sum of squares for the ABC interaction, and so on. The ANOVA decomposition for a 3-factor model is given by

$$SST = SS(A) + SS(B) + SS(C) + SS(AB) + SS(AC) + SS(BC) + SS(ABC) + SS(E) \quad (4.5)$$

where SST (the total sum of squares) measures the total variation in the response data and SSE (the error sum of squares) is the variation from all sources *other* than the factors included in the experiment [21].

4.3 Simulation Equipment

The equipment used to execute the simulations is a Dell Precision T7400 Workstation with the following system capabilities:

- Processor - Intel(R) Xeon(R) X5482 @ 3.20GHZ (2 processors)
- Memory (RAM) - 24.0 GB
- Operating System - 64-bit Windows 7
- Simulator - OPNET Modeler 15.0

4.4 Metrics for Performance Evaluation and Analysis

The following system metrics were chosen to evaluate the impact on MANET performance when RIPSec is implemented.

4.4.1 Total Route Errors Sent. This metric is a global statistic covering the entire scenario. It represents the total number of route error packets sent by all nodes in the network. This is a "Lower is Better" metric.

4.4.2 Load. This metric is a global statistic covering the entire scenario (50 nodes). It represents the total data traffic (in bits/second) received by the entire scenario from the higher layers of the Medium Access Control (MAC) that is accepted and queued for transmission. This statistic does not include any higher layer data

traffic that was rejected without queuing due to a full queue or large size of the data packet. Any data traffic that is relayed by a node from its sender to its receiver within the scenario is counted twice for this statistic (once at the sender node and once at the relay node). Such data packets are double-loads for the scenario because both the sender node and the relay node have to contend for their transmissions via the shared medium. If RIPSec is effective, error-prone nodes are avoided and less data traffic has to be retransmitted, thus decreasing the load on the network. This is a "Lower is Better" metric.

4.4.3 Throughput. This metric is a global statistic covering the entire scenario. It represents the total number of bits (in bits/second) forwarded from the wireless LAN layers to higher layers in all wireless nodes of the network. This is a "Higher is Better" metric.

4.5 Simulation Model Validation

In order to validate that the OPNET simulator being used was performing appropriately, simulations were configured and conducted according to previous research in this area [60]. The results were compared to the data provided in that research. Although using the AODV protocol, this validation reference was used because its configuration was very similar to RIPSec's and enough data was provided in the publication to make a comparison of the frameworks possible. The DSR model used as a reference for the simulation parameters did not serve as an acceptable validation source because the model could not be accurately reproduced to the extent a valid comparison was possible. Though not an ideal situation, the OPNET simulator was configured with AODV parameters and tested as explained in the next section.

4.5.1 Model Validation Implementation. The basic implementation of the AODV model used for validation includes the parameter settings defined in Table 4.4. The performance metrics are the routing overhead, defined as the amount of routing traffic sent in bits/second in the entire network and the delay, representing

the end-to-end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.

Table 4.4: Validation Workload Parameter Settings [60]

Workload Parameter	**Setting**
Simulation Time	3600 seconds
Ad Hoc Protocol	AODV
Node Distribution	Random
Nodes in Simulation	20
Sender Node	Fixed FTP Server Node
Receiver Nodes	20 Mobile Nodes
Application Load	Heavy FTP
Node Speed	Constant 10 meters per sec
Node Pause Time	300 sec
Simulation Area	1000 meters x 1000 meters
Transmission Range	250 meters
Mobility Model	Default Random Waypoint
FTP Clients	WLAN Mobile Nodes
Data Rate	11 Mbps
Transmission Power	0.005 watts

4.5.2 Model Validation Results. As can be seen in Figure 4.1, most of the data points from the referenced research implementing AODV were within the 95% confidence interval of the data points derived from the OPNET simulator used for this research. The data points from previous research shown in this figure are approximate because only the resulting graph was provided in the publication. However, the two sets of data points are nearly statistically equivalent. The actual data used to produce this figure is listed in Appendix B, Table B.1. The x-axis represents the length of the simulation, which was 3600 seconds. Each unit of measurement is approximately 82 seconds. The y-axis represents the packets sent per unit of time in bits/second.

Figure 4.2 shows the End-to-End delay in seconds of packets traversing the MANET. The referenced data falls within the 95% confidence interval of the data derived from the OPNET simulator used for this research, thus making it statistically equivalent. The data used to produce this figure is listed in Appendix B, Table B.2.

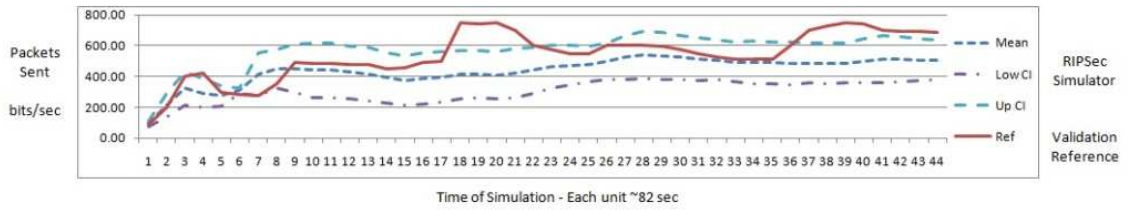

Figure 4.1: Routing Overhead in AODV

The x-axis represents the length of the simulation, which was 3600 seconds. Each unit of measurement is approximately 80 seconds. The y-axis represents the average delay per unit of time in seconds.

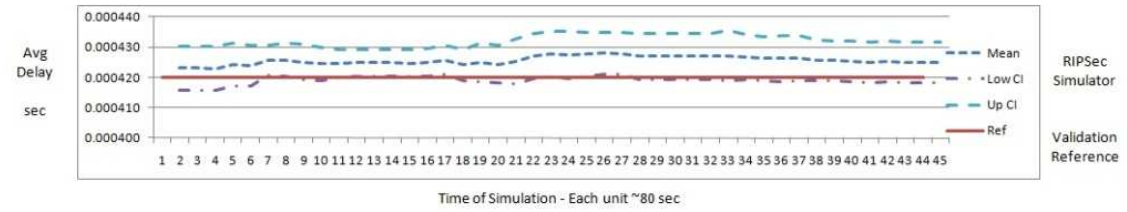

Figure 4.2: End-to-End Delay in AODV

The comparison of the OPNET simulator results to previously published research in MANETs confirms the model used is valid.

4.6 Summary

This chapter described the design methodology of the proposed RIPSec framework. It detailed the simulation environment, architecture models, and simulation equipment used. It also described the model's validation results. Chapter 5 presents an analysis of the performance results.

5. Simulation Results

5.1 Chapter Overview

This chapter presents the simulation results for RIPSec. The following section presents the results of RIPSec's impact on a MANET's load, throughput, and errors sent. Section 5.3 evaluates the diagnostics for residuals. Sections 5.4 presents an analysis of the simulation data. Section 5.5 provides a prediction expression that can be used to calculate the load, throughput, and errors sent given any value for the factors RIPSec on-off, number of misbehaving nodes, and percentage of misbehavior. The chapter concludes with a summary in Section 5.6.

5.2 RIPSec Performance

This section presents the simulation performance results. Table 5.1 enumerates the 12 groups of simulations used in this study. Groups A, C, E, G, I, and K are not RIPSec enabled while groups B, D, F, H, J, and L are RIPSec enabled.

Table 5.1: Simulation Groups

Group	**# Nodes**	**# Misbehaving**	**% Misbehaving**	**Ripsec**
A	50	10	10	Off
B	50	10	10	On
C	50	10	50	Off
D	50	10	50	On
E	50	25	10	Off
F	50	25	10	On
G	50	25	50	Off
H	50	25	50	On
I	50	40	10	Off
J	50	40	10	On
K	50	40	50	Off
L	50	40	50	On

Analysis of the results confirms RIPSec reduces the number of route errors sent in the MANET by an average of 53% (Figure 5.1, Table 5.2) while reducing the network load by an average of 18% (Figure 5.2, Table 5.3). Further analysis

demonstrates network throughput (Figure 5.3, Table 5.4) is reduced by an average of 34%, but is still sufficient to operate video conferencing applications. Groups A, C, E, G, I, and K are not RIPSec enabled while groups B, D, F, H, J, and L are RIPSec enabled.

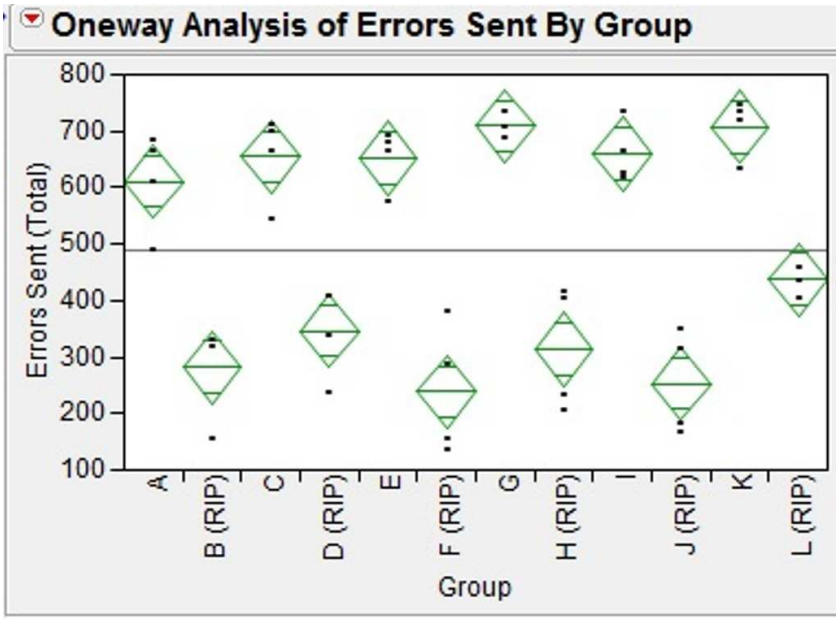

Figure 5.1: Analysis of Errors Sent By Group

Table 5.2: Percentage Change in Errors Sent By Group

Group w/o Ripsec Total Errors	**Group with Ripsec Total Errors**	**% Change**
A (611.11)	B (282.16)	-54%
C (654.90)	D (346.42)	-47%
E (651.95)	F (238.82)	-63%
G (708.69)	H (313.92)	-56%
I (659.90)	J (253.37)	-62%
K (707.41)	L (437.56)	-38%
	Average	-53%

Reduction of route errors sent can be attributed to RIPSec avoiding the use of nodes that are error prone. Reduction in network load can be attributed to the distribution of the load over several routes that are more likely to pass data from

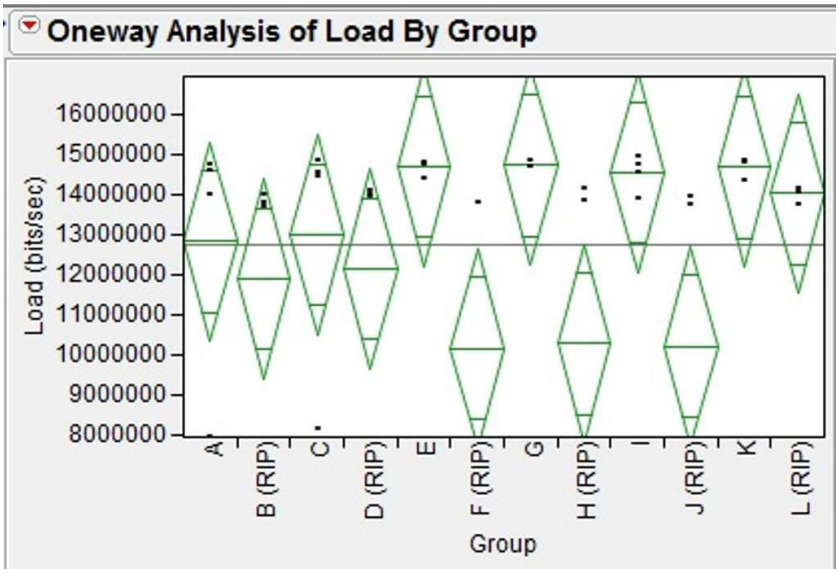

Figure 5.2: Analysis of Load By Group

Table 5.3: Percentage Change in Load By Group

Group w/o Ripsec bits/sec	**Group with Ripsec bits/sec**	**% Change**
A (12827168)	B (11908714)	-7%
C (13004017)	D (12145771)	-6%
E (14691356)	F (10173975)	-31%
G (14732423)	H (10279502)	-30%
I (14539108)	J (10217452)	-30%
K (14681401)	L (14032452)	-4%
	Average	-18%

Table 5.4: Percentage Change in Throughput By Group

Group w/o Ripsec bits/sec	**Group with Ripsec bits/sec**	**% Change**
A (4627654)	B (3537375)	-23%
C (4715165)	D (3235475)	-31%
E (4866663)	F (2981248)	-39%
G (4944898)	H (3005740)	-39%
I (4833506)	J (3068413)	-36%
K (4882259)	L (3212544)	-34%
	Average	-34%

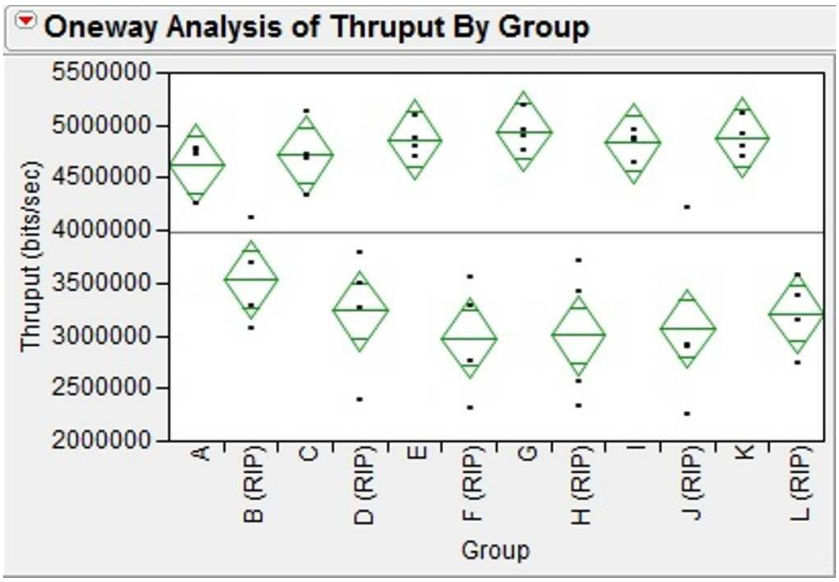

Figure 5.3: Analysis of Throughput By Group

sender to receiver nodes. Finally, reduction in network throughput can be attributed to the increase in packet size of a RIPSec enabled network and the extra round-trip time a packet takes to traverse the longer routes in the MANET. Throughput is defined as:

$$throughput = \frac{packet\ size}{time} \tag{5.1}$$

When RIPSec is enabled, the packet sizes increase from 64 to 96 bytes due to IPSec encapsulating the original packet and adding new header information. Additionally, the time for packets to traverse the MANET increases, dependent on the length of the multiple routes used by RIPSec. A simple example illustrates how this can happen. Without RIPSec, a packet size of 64 bytes and an average traversal time of 0.22 seconds (estimated from analysis) yields a calculated throughput of:

$$\begin{aligned} throughput &= \frac{64\ bytes}{0.22\ seconds} \\ throughput &= 291\ bytes/second \end{aligned} \tag{5.2}$$

Then, with RIPSec enabled, a packet size of 96 bytes and an estimated average traversal time of 0.30 seconds (estimated from analysis) yields a calculated throughput of:

$$\begin{aligned} throughput &= \frac{96\ bytes}{0.35\ seconds} \\ throughput &= 274\ bytes/second \end{aligned} \tag{5.3}$$

This section provided an overview of RIPSec's performance. The next section presents diagnostics for the residuals to determine if a linear regression model is appropriate.

5.3 Diagnostics for Residuals

When a regression model is selected for an application, it is important to examine the appropriateness of the model before further analysis is undertaken. In this section, the residuals are examined through diagnostics for the dependent variable. Residuals are defined as the difference between the observed and fitted values [57]. Residuals are assumed to be independent normal random variables, with mean 0 and constant variance σ^2. If the model is appropriate for the data at hand, the observed residuals should reflect these properties.

5.3.1 Residuals by Predicted Plot. The "Residual by Predicted Plot" graph displays the residual values by the predicted values of Y. This plot visually indicates if the residuals have a constant variance around the mean. Outliers are easily identified and may indicate a problem with the data. If the points in the graph trace out a U shaped pattern or an inverted U, there are nonlinear effects that have not been incorporated into the model.

5.3.1.1 Errors Sent Residual by Predicted Plot. Analysis of the errors sent residual in Figure 5.4 indicates the residual values are scattered around the mean.

The spread of the residuals appears to be constant over the range of predicted values and there are no outliers. Additionally, there is no U or inverted U shape to indicate nonlinearity. There are apparently two groups of data, explained by the binary nature of RIPSec (RIPSec is on or off).

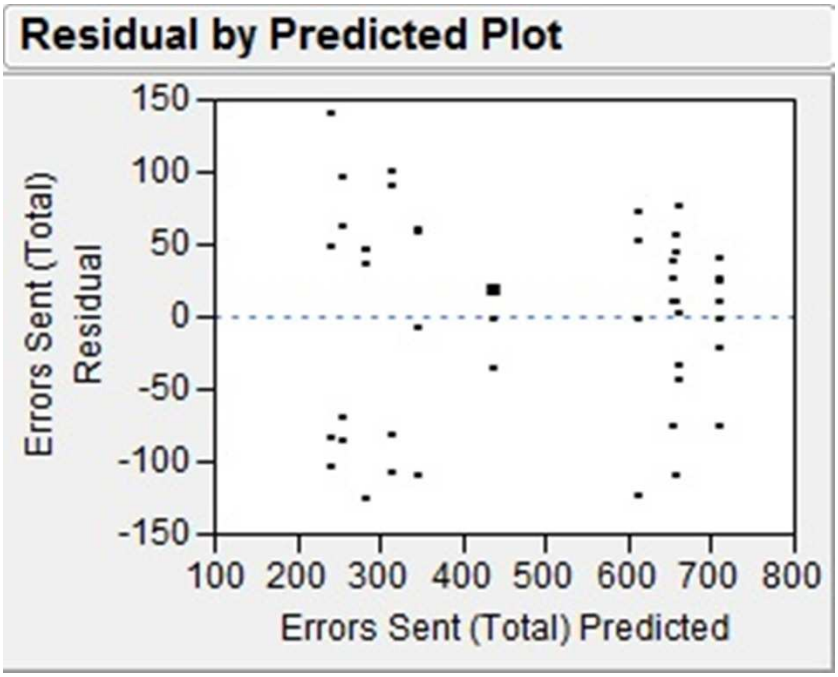

Figure 5.4: Errors Sent Residual by Predicted Plot

5.3.1.2 Load Residual by Predicted Plot. Analysis of the load residual in Figure 5.5 indicates the residual values are scattered around the mean. There is a definite pattern to the distribution of the residuals, but it is not U or inverted U shaped to indicate nonlinearity. Once again, there are two distinct groups of residuals, caused by enabling RIPSec. There are no outliers.

5.3.1.3 Throughput Residual by Predicted Plot. Figure 5.6 indicates the throughput residual values are scattered around the mean. There is again a definite pattern to the distribution of residuals, but it is not U or inverted U shaped to indicate nonlinearity. The binary nature of RIPSec creates the two groups of residuals.

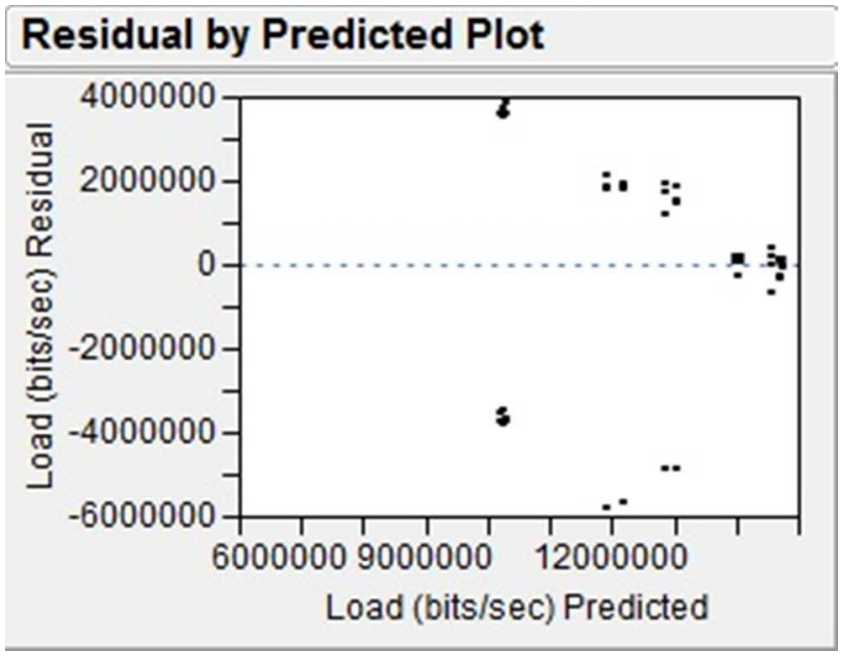

Figure 5.5: Load Residual by Predicted Plot

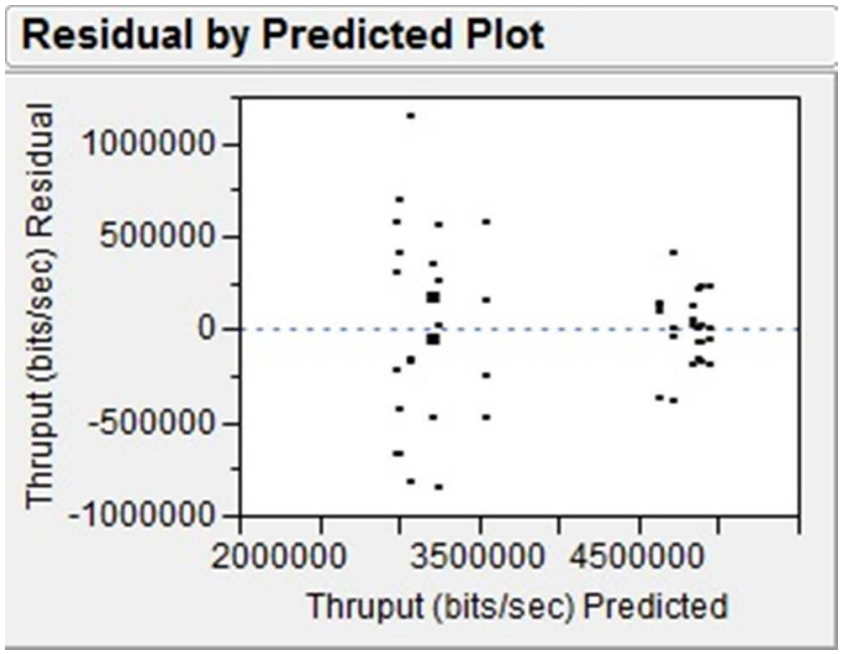

Figure 5.6: Throughput Residual by Predicted Plot

5.3.2 Diagnostics for Residuals Summary. The residuals of the data collected during simulation runs indicate the data is linear. Tests for normality are performed on the residuals with RIPSec disabled and enabled because the residuals

are separated into two groups for each metric (errors sent, load, and throughput). Tests for normality with RIPSec enabled and disabled indicate normally distributed residuals with the exception of load and is summarized in Table 5.5. In the table, a high W (Wilk) value is desirable.

Table 5.5: Goodness-of-Fit Test (Shapiro-Wilk W Test)

Distribution	**RIPSec**	**W Value**	**Prob < W**
Errors Sent	Disabled	0.9071	0.0306
Errors Sent	Enabled	0.9209	0.0613
Load	Disabled	0.4275	< 0.0001
Load	Enabled	0.6389	< 0.0001
Throughput	Disabled	0.9321	0.1088
Throughput	Enabled	0.9651	0.5496

The null hypothesis of the normal distribution test is that the data indeed comes from a normal distribution. Small p values (Prob ¡ W) indicate that the hypothesis of normality of the residuals should be rejected. If the residuals are not normal, as is the case with the load residuals, the estimates of the regression coefficients are still unbiased and have small variances, but the factors used in RIPSec are not good predictors of the network load and the hypothesis that the load is normally distributed must be rejected.

This section presented diagnostics to verify that the model used was linear and the residuals were normally distributed. The next section presents an analysis of the model results.

5.4 Data Analysis

This section utilizes the Actual by Predicted Plot, the Variance Inflation Factors (VIF), and the Analysis of Variance (ANOVA) to present the results of RIPSec.

5.4.1 Actual by Predicted Plot. The points on a leverage plot for simple regression are actual data coordinates, and the horizontal line for the constrained model is the sample mean of the response as shown in Figure 5.7.

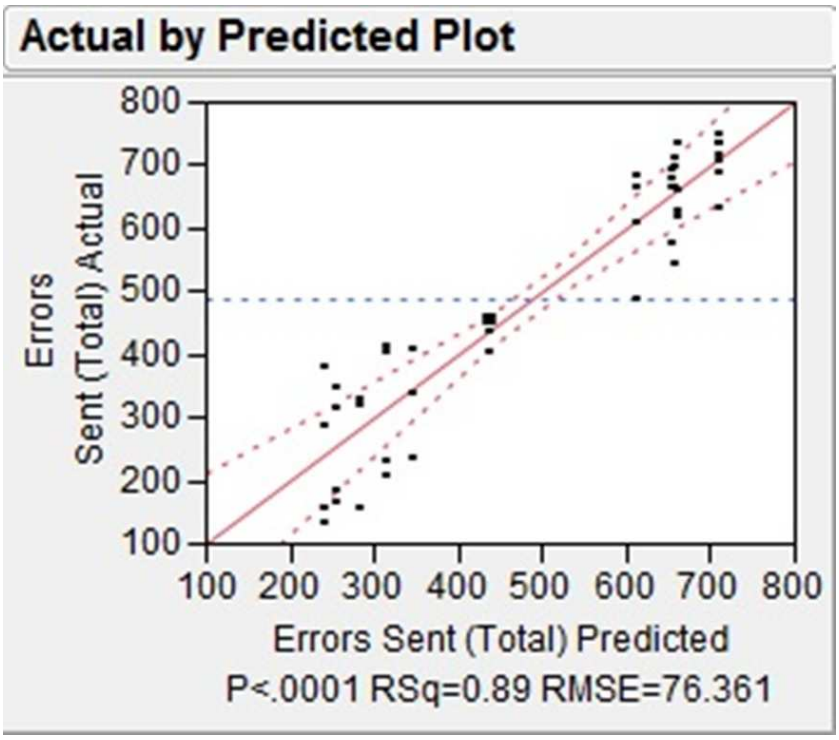

Figure 5.7: Example Actual by Predicted Plot

When the leverage plot is for one of multiple effects, as is the case here, the points are no longer actual data values. The horizontal line then represents a partially constrained model instead of a model fully constrained to one mean value. However, the intuitive interpretation of the plot is the same whether for simple or multiple regression. The idea is to judge if the line of fit on the effect's leverage plot carries the points significantly better than does the horizontal line [30].

Leverage plots are shown with confidence curves. These indicate whether the test is significant at the 5% level by showing a confidence region for the line of fit. If the confidence region between the curves contains the horizontal line, then the effect is not significant. If the curves cross the line, the effect is significant.

For continuous (versus discrete) responses, the Actual by Predicted plot shows how well it is fit. Each leaf is predicted with its mean, so the x-coordinates are these means. The actual values form a scatter of points around each leaf mean. A diagonal

line represents the set of point where predicted and actual values are the same. For a perfect fit, all the points would be on this diagonal [30].

The Actual by Predicted Plot function calculates three values of importance, the p-value, RSquare (RSq), and the Root Mean Square Error (RMSE) values.

- F-ratio is the model mean square divided by the error mean square. The underlying hypothesis of the fit is that all the regression parameters (except the intercept) are zero. If this hypothesis is true, then both the mean square for error and the mean square for model estimate the error variance, and their ratio has an F-distribution. If a parameter is a significant model effect, the F-ratio is usually higher than expected by chance alone. Probability > F is the observed significance probability (p-value) of obtaining a greater F-value by chance alone if the specified model fits no better than the overall response mean. P-values of 0.05 or less are often considered evidence of a regression effect and are statistically significant.
- RSq measures the proportion of the variation around the mean explained by the linear model. The remaining variation is not explained by the model and attributed to random error. RSq is 1 if the model fits perfectly. An RSq of 0 indicates the fit is not better than the simple mean model.
- RMSE estimates the standard deviation of the random error. It is the square root of the mean square for error in the Analysis of Variance Tables.

  The following sections will utilize the RSq values to determine how much of the variation around the mean is explained by the model. The three factors used in this model are: Number of Misbehaving Nodes, Percentage of Misbehavior, and RIPSec.

5.4.1.1 Actual by Predicted Plot for Errors Sent. In Figure 5.8, the Actual by Predicted Plot for errors sent indicates a very high proportion of the variation around the mean is explained by the model. Of the total variation, 89% is

explained by the selected factors. Therefore, this model is a very good predictor of the errors sent in a MANET.

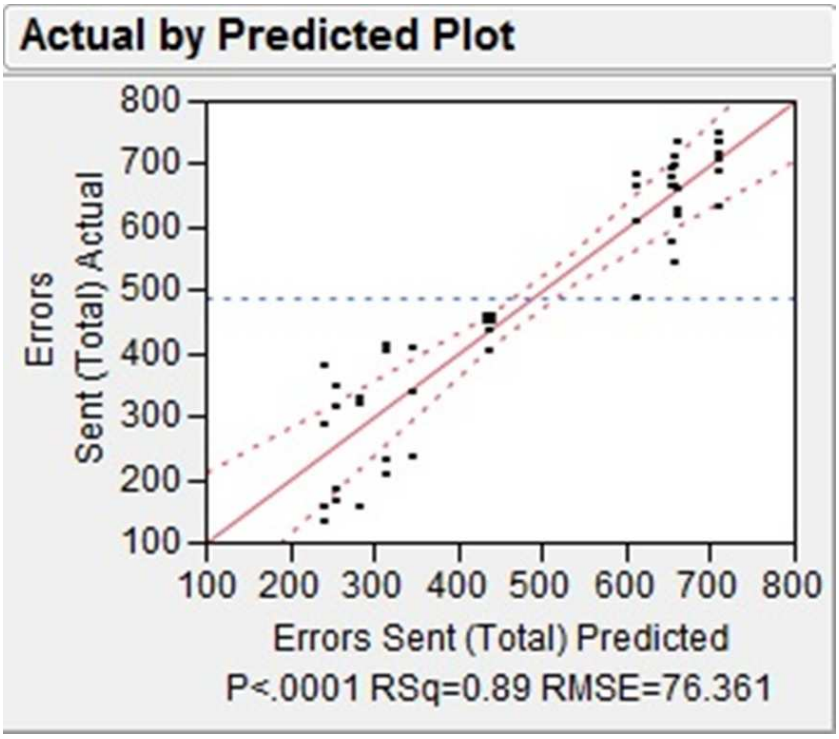

Figure 5.8: Actual by Predicted Plot for Errors Sent

Table 5.6 details the levels of significance of each regression factor to the model. Of the three factors, RIPSec had the most impact by far with a P-value of < 0.0001.

Table 5.6: Individual Factors' P-values for Errors Sent

Factor	**P-value**
RIPSec	< 0.0001
Num Misbehaving	0.1368
% of Misbehavior	0.0009

5.4.1.2 Actual by Predicted Plot for Load. In Figure 5.9, the Actual by Predicted Plot for Load indicates a very low proportion of the variation around the mean is explained by the model. Of the total variation, only 32% is explained by the selected factors. Though better than a simple mean model, the RIPSec framework and factors varied are not a good predictor of the network load in a MANET.

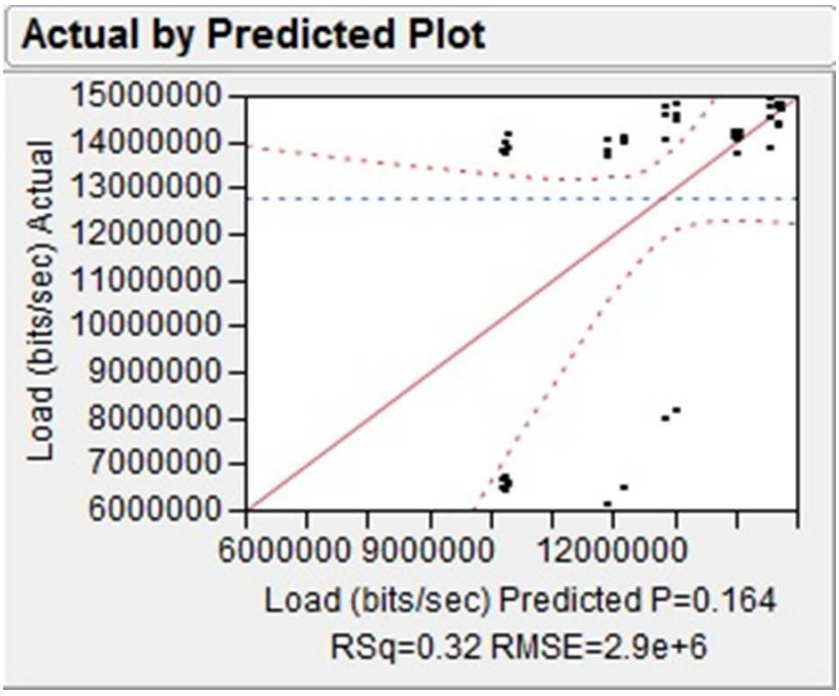

Figure 5.9: Actual by Predicted Plot for Load

Table 5.7 details the levels of significance of each regression factor to the model. Of the three factors, RIPSec had the most impact with a P-value of 0.0029.

Table 5.7: Individual Factors' P-values for Load

Factor	**P-value**
RIPSec	0.0029
Num Misbehaving	0.3829
% of Misbehavior	0.3693

5.4.1.3 Actual by Predicted Plot for Throughput. In Figure 5.10, the Actual by Predicted Plot for Throughput indicates a high proportion of the variation around the mean is explained by the model. Of the total variation, 82% is explained by the selected factors indicating the RIPSec model was a very good predictor of throughput for a MANET.

Table 5.8 details the levels of significance of each regression factor to the model. Of the three factors, RIPSec had by far the most impact with a P-value of < 0.0001.

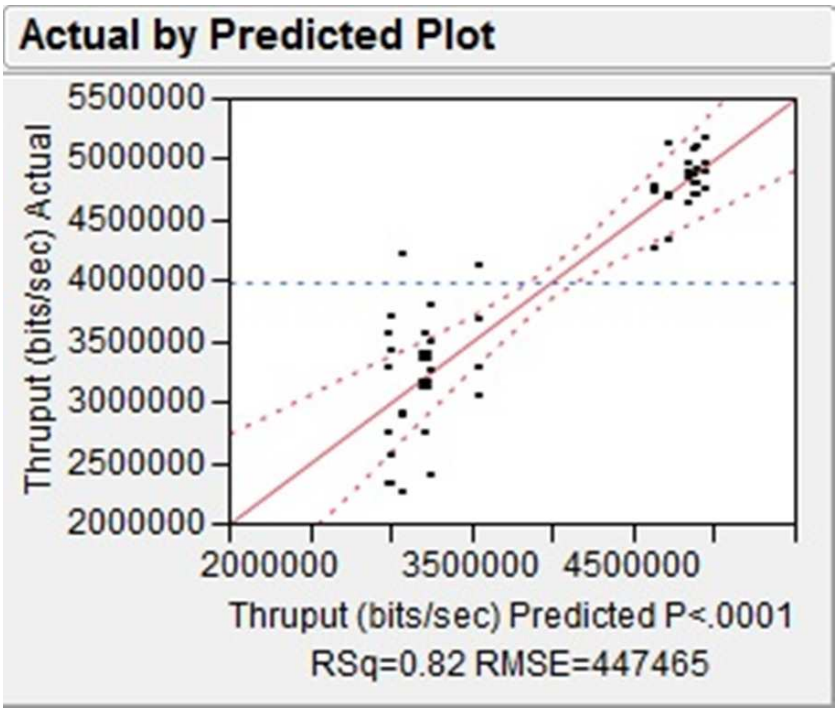

Figure 5.10: Actual by Predicted Plot for Throughput

Table 5.8: Individual Factors' P-values for Throughput

Factor	**P-value**
RIPSec	< 0.0001
Num Misbehaving	0.8476
% of Misbehavior	0.9147

5.4.2 Variance Inflation Factors (VIF). The VIFs are useful in determining which variables may be correlated or collinear. For the ith independent variable, the VIF is defined as

$$\frac{1}{1 - R_i^2} \tag{5.4}$$

where R_i^2 is the coefficient of determination for the regression of the ith independent variable on all other independent variables. High VIFs indicate a collinearity problem. VIFs of 1 indicate no collinearity. As can be seen in Figure 5.11, there are no collinearity problems with the RIPSec model.

Parameter Estimates

Term	Estimate	Std Error	t Ratio	Prob>|t|	VIF
Intercept	572.62034	31.97631	17.91	<.0001*	.
Num Misbehaving	1.3637824	0.899938	1.52	0.1368	1
% of Misbehavior	1.9649036	0.551097	3.57	0.0009*	1
RIPSEC	-353.6198	22.04389	-16.04	<.0001*	1

Figure 5.11: Variance Inflation Factors

5.4.3 Analysis of Variance (ANOVA). ANOVA for a linear regression partitions the total variation of a sample into components. These components are used to compute an *F-ratio* that evaluates the effectiveness of the model. If the probability associated with the *F-ratio* is small, then the model is considered a better statistical fit for the data than the response mean alone. The ANOVA table displays the following quantities: *Source* lists the three sources of variation, *Model*, *Error*, and *C. Total*. *Degrees of Freedom* (DF) records the associated degrees of freedom for each source of variation. *Sum of Squares* records an associated sum of squares (SS for short) for each source of variation. *Mean Square* is a sum of squares divided by its associated degrees of freedom.

F Ratio is the model mean square divided by the error mean square. The underlying hypothesis of the fit is that all the regression parameters (except the intercept) are zero. If this hypothesis is true, then both the mean square for error and the mean square for model estimate the error variance, and their ratio has an F-distribution. If a parameter is a significant model effect, the *F-ratio* is usually higher than expected by chance alone.

Prob > *F* is the observed significance probability (p-value) of obtaining a greater F-value by chance alone if the specified model fits no better than the overall response mean. Observed significance probabilities of 0.05 or less are often considered evidence of a regression effect.

5.4.3.1 Analysis of Variance for Errors Sent. In Figure 5.12, the Analysis of Variance for errors sent has a high F Ratio of 90.78 and a very low Prob > F of <0.0001, indicating errors sent is a significant model effect.

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio
Model	3	1588082.7	529361	90.7808
Error	44	256572.7	5831	Prob > F
C. Total	47	1844655.4		<.0001*

Figure 5.12: ANOVA for Errors Sent

5.4.3.2 Analysis of Variance for Load. In Figure 5.13, the Analysis of Variance for Load has a very low F Ratio of 3.8527 and a marginal Prob > F of 0.0156, indicating load is not a significant model effect. In fact, load provides only a slightly better possibility of obtaining a greater F-value than by chance alone.

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio
Model	3	9.5576e+13	3.186e+13	3.8527
Error	44	3.6385e+14	8.269e+12	Prob > F
C. Total	47	4.5943e+14		0.0156*

Figure 5.13: ANOVA for Load

5.4.3.3 Analysis of Variance for Throughput. In Figure 5.14, the Analysis of Variance for Throughput has a respectable F Ratio of 56.7059 and a very low Prob > F of <0.0001, indicating throughput is a significant model effect.

5.4.4 Data Analysis Summary. This section provided an analysis of the data collected through RIPSec simulations. The analysis indicates RIPSec has a significant effect on the number of errors sent and on the throughput in a MANET,

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio
Model	3	3.2215e+13	1.074e+13	56.7059
Error	44	8.3321e+12	1.894e+11	Prob > F
C. Total	47	4.0547e+13		<.0001*

Figure 5.14: ANOVA for Throughput

but it does not have a significant effect on the network load. These are desirable results and demonstrate the RIPSec framework is a viable solution for providing security of nodes through encryption, behavior grading through the reputation indexes, and load balancing through multipath routing while still providing sufficient throughput to support Video Conferencing applications operating at a medium load level. The next section presents the regression model that can be used to predict the system metrics of errors sent, load, and throughput given arbitrary values for the selected factors of RIPSec on or off (0,1), number of misbehaving nodes, and percentage of misbehavior.

5.5 Prediction Expression

One application of a multiple regression model is the ability to make a valid projection concerning an outcome for a particular individual prediction. The goal is to use the prediction equation to predict outcomes for factors not in the sample used in the analysis. The prediction equation is created by gathering relevant data from a large, representative sample from the population. The actual sample size is debatable, but the larger the sample, the better the prediction expression. Only variables that contribute significantly to the variance accounted for by the regression equation are included.

- For the metric errors sent, the prediction expression is $(572.6203) - (353.6197 \times RIPSec(0,1)) + (1.3638 \times NumMisbehaving) + (1.9649 \times \%\ of Misbehavior)$.

- For the metric load, the prediction expression is $(1.2767) - (2619 \times RIPSec(0,1)) + (29872.8612 \times NumMisbehaving) + (18824.1401 \times \%\ of Misbehavior)$.
- For the metric throughput, $(4826318.8856) - 1638224.9737 \times RIPSec(0,1)) - (991.2331 \times NumMisbehaving) + (338.4206 \times \%\ of Misbehavior)$ is the prediction expression.

5.6 Summary

This chapter presented an analysis of the results from this research. An overview of RIPSec's impact on the model was presented followed by the diagnostics for residuals. An analysis of the data showed RIPSec had significant effects on the number of errors sent and on throughput while minimal effects on load. Finally, the prediction expressions for each metric were presented. The next chapter summarizes this research.

6. RIPSec Analysis

6.1 Chapter Overview

Chapter 5 presented performance results for RIPSec, showing its multiple security layers provides a secure and functional MANET. This chapter presents further discussion of the protocol. Section 6.2 describes the engineering advantages of using RIPSec, and Section 6.3 describes the effectiveness of RIPSec against various MANET attacks. The chapter concludes with a summary in Section 6.4.

6.2 Engineering Advantages of RIPSec

RIPSec is designed to be a complete multilevel security framework that is resistant to numerous MANET attacks. Its unique design affords many engineering advantages, to include:

- A framework that is extremely resistant to numerous types of network-based attack, from both external and internal threats, due to the particular implementation of IPSec used (PKI device certificates and transport ESP mode). Transport mode is rarely used when IPSec is deployed because most implementations are only concerned with encryption of data. In those instances, IPSec tunnel mode is used. However, transport mode is very effective at protecting individual nodes from unauthorized access. PKI device certificates deployed in transport ESP mode ensure integrity of data, confidentiality, authenticity, and anti-replay protection.
- A framework that is extremely resistant to node misbehavior (intentional or not) due to the behavior grading/reputation mechanism employed.
- A framework that is not susceptible to common IPSec attacks based on PKI key distribution weaknesses because the PKI device certificates are distributed out-of-band. The only known attacks against IPSec are against the key distribution mechanism.

- A framework that minimizes dependence on single nodes/routes by using multiple routes to a receiver node without increasing the number of packets introduced into the network.

6.3 Effectiveness of RIPSec Against MANET Attacks

This section describes the most common attacks against MANETs [84] and provides an analysis of how successful they might be against RIPSec.

6.3.1 Eavesdropping. Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. Nodes in a MANET share a wireless medium. The majority of wireless communications use the Radio Frequency (RF) spectrum where broadcast signals can be easily intercepted with receivers tuned to the proper frequency [41] [59]. Therefore, messages transmitted can be eavesdropped, and fake messages can be injected into the network.

Eavesdropping attacks are stopped in RIPSec because data is encrypted with PKI certificates and only the receiver node can interpret the data correctly.

6.3.2 Routing Table Overflow. A malicious node may advertise routes that do not exist in an attempt to overflow the routing table of a victim node. The attacker tries to create enough routes to prevent new routes from being created. Proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover complete routing information to all nodes before it is actually needed.

RIPSec is not vulnerable to this attack because it is a reactive routing algorithm and only requests new routes when it needs them. Additionally, only routes containing nodes with neutral or higher RIs are maintained by sender nodes, thus reducing the total number of routes maintained in the route cache and reducing the likelihood of an overflow condition.

6.3.3 Routing Cache Poisoning. Attackers may take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. If a malicious node wants to poison routes to another node, the malicious node could broadcast spoofed packets with a source route to the receiver node from itself. All neighboring nodes that overhear the packet may add the invalid spoofed route to their route caches.

RIPSec would be less vulnerable to this attack because it would not update its route cache unless a new route was requested, or a route needed to be eliminated from the cache because one of the nodes in the route obtained a negative RI. When requesting a new route, a malicious node could answer with an invalid route, but the route would be eliminated when the missing nodes earned negative reputations for failing to acknowledge and relay packets. Additionally, RIPSec is less dependent on any one route due to the round-robin multipath routing of packets. Note that all of the reviewed security frameworks are vulnerable to this attack.

6.3.4 Routing Maintenance. Attacks may target the route maintenance phase of a protocol such as DSR and AODV by broadcasting false control messages, such as link-broken error messages, which starts in motion the process of deleting supposedly broken routes and the discovery of new routes.

RIPSec is vulnerable to this attack because it depends on route error messages to adjust nodes' RI. If the error notification mechanism of the DSR protocol is compromised, RIPSec-generated RIs will be invalid. This particular attack is difficult for a reputation-based system to defend against and is recommended as future work. Note that all of the reviewed security frameworks are vulnerable to this attack.

6.3.5 Data Forwarding. Malicious nodes may participate cooperatively in the routing protocol discovery and maintenance phases, but in the data forwarding

phase they do not forward data packets consistently. They may simply drop packets quietly, modify data content, replay, or flood data packets.

RIPSec is very effective at combating this attack. A node sending data to a relay node listens to ensure the relay node forwards the data to next node in the route. If the sending node detects the data was not forwarded, it generates a route error and the RI of the offending relay node is adjusted accordingly. Once the offending node's RI becomes negative, it is avoided in the route selection process.

6.3.6 Wormhole. An attacker may accept packets, but then tunnel them to another location. Wormhole attacks are severe threats to MANET routing protocols. This attack could prevent the discovery of any routes other than through the wormhole.

This attack cannot be successful against RIPSec because nodes can only communicate with the other nodes in the MANET which have PKI certificates and security associations. Without a security association, communication simply cannot take place. Even if data is sent to another node in the MANET, the data is not discernible by any other node other than the receiver.

6.3.7 Sinkhole. This sinkhole attack has two phases. The attacker advertises itself as having a valid route to a receiver, even though the node only intends to intercept packets. Then, the attacker consumes the intercepted packets without any forwarding, or at best, selectively forwarding the packets. An attacker may also consume packets from some source while correctly forwarding packets from other sources, thus limiting the suspicion in the MANET.

RIPSec is effective at stopping this attack because packets that are not relayed cause the RI of the attacker to be decremented. It is not beneficial for an attacker to gather packets for data analysis because the data cannot be discerned by anyone other than the intended node.

6.3.8 Byzantine. A compromised relay node, or a set of compromised relay nodes, may carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets. These actions result in the disruption or degradation of routing services.

RIPSec combats these attacks by using more than one route to a receiver node. If enough nodes in the MANET participated in this type of attack, performance would be impacted significantly. The behavior grading scheme would detect the dropping of packets and adjust RIs accordingly.

6.3.9 Selfish Nodes. In this attack, nodes drop relay packets with the intention of greedily using the wireless medium for sending their own source packets. Another motivation for this attack may be to save battery power, but the end result is the same. Selfish nodes are not conducive to the overall MANET.

RIPSec is effective at detecting and isolating selfish nodes through its behavior grading mechanism. If nodes do not forward packets, their RI is decremented and when it becomes negative, the selfish node is avoided in future route requests. If the selfishness is for legitimate reasons (e.g., conserving battery power), the action taken is the best approach as the selfish node may still be able to function in the MANET without becoming unusable.

6.3.10 External Denial of Service. A node external to the trusted MANET may attempt to flood a particular node with packets and requests for service in an attempt to occupy all the victim node's resources and thus prevent the victim from participating in the MANET.

This attack is stopped in RIPSec by the implementation of IPSec. A node external to the MANET does not have a security association with any node in the MANET, and without a security association, no communication can take place. No processing resources of the victim will be used as packets are denied at the network level.

6.3.11 Internal Denial of Service. One of the trusted nodes in the MANET may attempt to tie up the resources of another node by flooding it with requests for service. RIPSec will detect any node that is so constrained and will avoid it when the RI becomes negative. Internal nodes have the capability of communicating freely with other internal nodes, so the actual denial of service is difficult to avoid. However, the adverse effect is minimized with RIPSec.

6.3.12 Spoofing. This attack is also known as an impersonation attack. A malicious node may hide its IP address and use that of another node to launch attacks. This attack is designed to isolate a valid node from the network and use its credentials in the network as an attack platform.

This attack is defeated in RIPSec because of the IPSec implementation. Security associations are established with nodes based on their PKI certificates in conjunction with their network addresses. Without a valid certificate, a security association cannot be established and communication cannot take place.

6.3.13 Sybil. A Sybil attack occurs when the reputation system is compromised by an attacker forging and creating large numbers of identities and then using them to gain a disproportionately large influence.

This attack is stopped in RIPSec because an identity cannot be spoofed due to the implementation of PKI certificates. Every node is unquestionably identifiable.

6.3.14 Badmouthing. A malicious node may generate numerous routing error messages in an attempt to harm the reputation of another node. This is an attack on the reputation system.

RIPSec does not stop this attack in its current configuration. Incorrect generation of error messages will subvert RIPSec's behavior grading mechanism. A solution to this attack is left for future research. Note that all of the reviewed security frameworks are vulnerable to this attack.

6.3.15 Flattering. A malicious node may attempt to increase the reputation of another node by falsely generating positive feedback items. This is an attack on the reputation system.

RIPSec stops this attack in the way a node's reputation is increased. Positive feedback items are generated when a relay node acknowledges receipt of a packet and then forwards the packet downstream. Unsolicited positive feedback as to a node's reputation is not accepted and is not a part of this framework. Positive feedback only comes in the form of acknowledgments and the passive detection of nodes forwarding data.

6.4 Comparison of RIPSec to Existing Frameworks

The existing frameworks described in Chapter 2 are compared to RIPSec to demonstrate this framework's effectiveness at securing a MANET. The results are summarized in Figure 6.1 and Figure 6.2.

Of the four features incorporated into RIPSec (encryption, IPSec transport mode, behavior grading, and multipath routing), three other frameworks incorporated two of the features (encryption and behavior grading), and the remaining eight frameworks only incorporated one security feature. The multiple security levels of RIPSec make it very robust against attacks.

Of the 15 MANET attacks reviewed, RIPSec is effective at mitigating 12. The other frameworks could only mitigate at best five attacks. This demonstrates RIPSec's effectiveness at combating a broad range of threats.

6.5 Chapter Summary

This chapter provides an analysis of RIPSec's effectiveness. The engineering advantages are presented along with RIPSec's ability to mitigate attacks compared with similar published MANET security frameworks. The next chapter provides a conclusion to this dissertation.

Framework	Reputation Based Internet Protocol Security (RIPSec)	Mobile Certification Authority (MOCA)	Maximum Degree Algorithm (MDA)	Self-Organized Network-Layer Security (SCAN)	Techniques for Intrusion Resistant Ad Hoc Routing Algorithms (TIARA)	Secure Efficient Ad hoc Distance Vector (SEAD)
Features						
Encryption	Yes	Yes	Yes	No	No	Yes
IPSec Transport Mode	Yes	No	No	No	No	No
Behavior Grading	Yes	No	No	Yes	Yes	No
Multipath	Yes	No	No	No	No	No
Attack Defense						
Eavesdropping	Yes	Yes	Yes	No	No	Yes
Routing Table Overflow	Yes	No	No	No	No	No
Routing Cache Poisoning	Partial	No	No	No	No	No
Routing Maintenance	No	No	No	No	No	No
Data Forwarding	Yes	No	No	Yes	No	No
Wormhole	Yes	No	No	Yes	No	No
Sinkhole	Yes	No	No	Yes	No	No
Byzantine	Yes	No	No	Yes	No	No
Selfish Nodes	Yes	No	No	No	No	No
External DoS	Yes	No	No	No	Yes	Yes
Internal DoS	Yes	No	No	No	Yes	Yes
Spoofing	Yes	Yes	Yes	No	No	No
Sybil	Yes	Yes	Yes	No	No	No
Bad Mouthing	No	No	No	No	No	No
Flattering	Yes	No	No	No	No	No
Total Attributes	12	3	3	4	2	3

Figure 6.1: RIPSec Comparison to Existing Frameworks Part 1

Framework	Reputation Based Internet Protocol Security (RIPSec)	On-demand Secure Routing Protocol (OSRP)	Alliance of Remote Instruction Authoring and Distribute Networks Europe (ARIADNE)	Security Aware Ad Hoc (SAR)	Collaborative Reputation Mechanism (CORE)	Cooperation Of Nodes: Fairness In Dynamic Ad Hoc Networks (CONFIDANT)	Watchdog and Pathrater
Features							
Encryption	Yes	Yes	Yes	Yes	No	Yes	No
IPSec Transport Mode	Yes	No	No	No	No	No	No
Behavior Grading	Yes	Yes	Yes	No	Yes	Yes	Yes
Multipath	Yes	No	No	No	No	No	No
Attack Defense							
Eavesdropping	Yes	Yes	Yes	Yes	No	No	No
Routing Table Overflow	Yes	No	No	No	No	No	No
Routing Cache Poisoning	Partial	No	No	No	No	No	No
Routing Maintenance	No	No	No	No	No	No	No
Data Forwarding	Yes	Yes	Yes	No	Yes	Yes	Yes
Wormhole	Yes	No	No	No	No	No	No
Sinkhole	Yes	No	Yes	No	No	No	No
Byzantine	Yes	Yes	No	No	No	No	No
Selfish Nodes	Yes	No	No	No	Yes	Yes	Yes
External DoS	Yes	No	No	No	No	No	No
Internal DoS	Yes	No	No	No	No	No	No
Spoofing	Yes	Yes	Yes	Yes	No	No	No
Sybil	Yes	Yes	Yes	Yes	No	No	No
Bad Mouthing	No	No	No	No	No	No	No
Flattering	Yes	No	No	No	No	No	No
Total Attributes	12	5	5	3	2	2	2

Figure 6.2: RIPSec Comparison to Existing Frameworks Part 2

7. Conclusion

7.1 Summary of Research

The goal of this research is to investigate how to integrate security policies of a MANET with behavior grading and encryption algorithms in a fashion that would allow the MANET to function securely in a hostile environment without degrading network performance.

7.2 Research Contributions

The technical contribution of this research is a framework, called Reputation-based IPSec (RIPSec), for securing a MANET operating in a hostile environment. It uses IPSec in transport mode to protect nodes from external threats. It uses behavior grading of nodes to calculate Reputation Indexes, which are used to select nodes used in the route discovery process. The Dynamic Source Routing (DSR) protocol is modified to utilize all discovered routes instead of the shortest route to balance the network load across multiple paths.

Results of this research were very promising. Analysis of the results confirmed RIPSec reduced the number of route errors sent in the MANET by an average of 53%, while reducing the network load by an average of 18%. Further analysis demonstrated network throughput was reduced by an average of 34%, but was still sufficient to operate video conferencing applications demonstrated by the completion of the simulations. During preliminary simulations, the video conferencing applications failed when throughput was insufficient to maintain communications between sender and receiver nodes.

The engineering advantages of RIPSec are:

- A framework that is extremely resistant to numerous types of network-based attack, from both external and internal threats, due to the particular implementation of IPSec used (PKI device certificates and transport ESP mode).

Transport mode is rarely used when IPSec is deployed because most implementations are only concerned with encryption of data. In those instances, IPSec tunnel mode is used. However, transport mode is very effective at protecting individual nodes from unauthorized access. PKI device certificates deployed in transport ESP mode ensure integrity of data, confidentiality, authenticity, and anti-replay protection.

- A framework that is extremely resistant to node misbehavior (intentional or not) due to the behavior grading/reputation mechanism employed.
- A framework that is not susceptible to common IPSec attacks based on PKI key distribution weaknesses because the PKI device certificates are distributed out-of-band. The only known attacks against IPSec are against the key distribution mechanism.
- A framework that minimizes dependence on single nodes/routes by using multiple routes to a receiver node without increasing the number of packets introduced into the network.

RIPSec incorporates four security features (encryption, IPSec transport mode, behavior grading, and multipath routing) into its framework while maintaining network performance sufficient to operate high bandwidth applications. Three other frameworks incorporate two of the features (encryption and behavior grading), and the remaining eight frameworks studied only incorporate one security feature.

The multiple security levels of RIPSec make it very robust against attacks. Of the 15 MANET attacks reviewed, RIPSec is effective at mitigating 12 of them. The other frameworks could only mitigate at best five of the attacks. This demonstrates RIPSec's effectiveness at combating a broad range of threats.

7.3 Recommendations for Future Research

The first area of future research should be to eliminate the few areas where RIPSec is vulnerable to attack, illustrated in Table 7.1. RIPSec should be hardened against route cache poisoning, route maintenance attacks, and bad mouthing attacks.

Table 7.1: RIPSec Areas of Improvement

Attack	**Mitigated**
Eavesdropping	Yes
Routing Table Overflow	Yes
Routing Cache Poisoning	Partial
Routing Maintenance	No
Data Forwarding	Yes
Wormhole	Yes
Sinkhole	Yes
Byzantine	Yes
Selfish Nodes	Yes
External DoS	Yes
Internal DoS	Yes
Spoofing	Yes
Sybil	Yes
Bad Mouthing	No
Flattering	Yes
Areas of Improvement	3

This research was conducted via simulation. One possible area of future research would be to implement this framework in a test bed of mobile network devices. The use of laptops in vehicles would certainly have the processing power and battery life to support the RIPSec framework. A good application in such an ad-hoc network would be the use of a video camera to surveil a person of interest, sending a live video feed to a command center. Multiple vehicles could be used to minimize the likelihood of detection.

Another area of future research is the use of RIPSec to secure ad-hoc networks of mobile sensors deployed in a hostile environment. These sensors are normally small

and resource constrained. The analysis of the impact RIPSec has on a small computer platform would be beneficial to determine the range of applicability of this framework.

A final area of future research would be the deployment of RIPSec into a large ad-hoc network to determine the scalability of the framework. It is anticipated the larger the network, the better RIPSec would perform, given more choices for nodes and routes would be available to a sender node. The management of neighbor nodes and their certificates would be the constraining factor and would be limited primarily by the operating memory of the nodes.

7.4 Concluding Thoughts

This particular research was pursued because the author believes there is a need for incorporating encryption technology, especially IPSec, into operational mobile networks. This research has demonstrated that it can be done and, if implemented correctly, can provide a much more secure operating environment than is currently being used.

Appendix A.

The following sections contain the source code modifications made in the OPNET Modeler simulator v15.0 to implement the RIPSec framework. Only the modules that were modified are included in this appendix. Actual source code changes may be obtained by contacting the author at the Air Force Institute of Technology.

A.1 IP Dispatch Function Block

A.1.1 IP Dispatch Do Init.

A.1.2 IP Dispatch Init Phase 2.

A.2 DSR Rte Function Block

A.2.1 DSR Rte Sv Init.

A.2.2 DSR Rte Stats Reg.

A.2.3 DSR Rte Received Pkt Handle.

A.2.4 DSR Rte Received Route Error Process.

A.2.5 DSR Rte Received Acknowledgement Option Process.

A.2.6 DSR Rte Route Error Send.

A.2.7 DSR Rte Jittered Pkt Send.

A.2.8 DSR Rte Route Cache Update.

A.3 DSR Route Cache

A.3.1 Declarations.

A.3.2 DSR Route Cache Entry Add.

A.3.3 DSR Route Cache Entry Access.

A.3.4 DSR Route Cache Path Get.

A.4 IP Rte Support Header

A.4.1 Declarations.

A.5 DSR Ptypes Header

A.5.1 Declarations.

Appendix B.

The following tables contain the simulation data.

B.1 AODV Routing Overhead Data for Model Verification

Table B.1: AODV Routing Overhead Data for Model Verification

Run 1 Sd 25	Run 2 Sd 128	Run 3 Sd 132	Run 4 Sd 150	Mean	St Dev	Conf Int	Low CI	Up CI	Rsrch	Horztl Axis
74.77	81.44	106.96	106.81	92.50	16.84	16.50	75.99	109.00	90.00	1.00
200.80	145.98	325.78	187.68	215.06	77.43	75.88	139.18	290.93	200.00	1.00
241.78	246.76	474.31	328.44	322.82	108.53	106.36	216.47	429.18	400.00	2.00
221.63	224.32	432.59	291.95	292.62	98.82	96.84	195.78	389.47	425.00	2.00
254.70	205.63	370.79	262.76	273.47	69.62	68.23	205.24	341.70	300.00	3.00
322.73	290.87	324.44	296.16	308.55	17.51	17.16	291.39	325.71	285.00	3.00
623.11	316.63	358.42	349.85	412.00	141.89	139.05	272.96	551.05	275.00	4.00
627.94	330.43	456.09	387.83	450.57	128.92	126.34	324.23	576.91	350.00	4.00
667.66	309.78	474.83	360.13	453.10	158.84	155.66	297.43	608.76	490.00	5.00
694.67	291.56	435.26	336.12	439.40	180.47	176.85	262.55	616.25	487.00	5.00
666.53	275.36	502.02	315.11	439.75	180.61	177.00	262.75	616.75	485.00	6.00
633.20	260.87	511.17	296.58	425.45	177.21	173.66	251.80	599.11	480.00	6.00
603.05	247.82	521.24	280.10	413.05	175.86	172.34	240.71	585.39	475.00	7.00
575.64	236.02	488.67	265.36	391.42	166.77	163.43	227.99	554.85	450.00	8.00
564.10	225.29	459.92	252.09	375.35	163.80	160.52	214.83	535.87	455.00	9.00
581.52	245.22	471.75	240.08	384.64	169.99	166.58	218.06	551.23	490.00	10.00
584.32	283.07	481.78	229.17	394.59	166.73	163.39	231.19	557.98	500.00	11.00
587.73	355.06	490.80	219.21	413.20	160.72	157.50	255.69	570.70	750.00	12.00
565.96	383.32	497.95	210.07	414.32	155.63	152.52	261.81	566.84	745.00	13.00
550.35	369.12	503.96	201.67	406.27	156.57	153.44	252.84	559.71	747.00	14.00
573.33	355.94	540.10	218.97	422.09	165.76	162.44	259.64	584.53	700.00	15.00
575.59	405.18	544.30	235.82	440.22	155.09	151.99	288.23	592.21	600.00	16.00
619.04	434.04	522.52	277.75	463.34	144.97	142.07	321.27	605.41	575.00	17.00
620.06	462.77	502.43	307.19	473.11	129.22	126.63	346.48	599.74	550.00	18.00
621.01	469.00	493.33	336.83	480.04	116.45	114.12	365.93	594.16	550.00	19.00
659.92	454.79	513.84	369.03	499.40	122.42	119.97	379.42	619.37	600.00	20.00
732.01	441.41	518.59	399.22	522.81	147.97	145.01	377.80	667.81	600.00	21.00
763.31	428.80	524.44	443.45	540.00	154.70	151.60	388.40	691.60	600.00	22.00
760.29	416.89	507.53	449.57	533.57	155.72	152.61	380.96	686.18	598.00	23.00
740.28	422.94	491.67	436.72	522.90	147.93	144.97	377.94	667.87	575.00	24.00
721.30	428.96	476.77	424.59	512.90	140.93	138.10	374.80	651.01	550.00	25.00
703.27	451.37	462.75	413.12	507.63	132.14	129.50	378.13	637.12	525.00	25.00
686.11	440.09	449.52	402.25	494.49	129.37	126.78	367.71	621.27	515.00	26.00
699.28	429.36	437.04	391.93	489.40	141.30	138.47	350.93	627.87	513.00	26.00
699.91	419.13	425.23	412.04	489.08	140.66	137.84	351.24	626.92	510.00	27.00
699.29	409.39	414.04	421.53	486.06	142.24	139.40	346.66	625.46	600.00	27.00
683.75	429.70	403.42	427.51	486.10	132.31	129.66	356.44	615.76	700.00	28.00
683.52	434.86	393.33	417.57	482.32	135.21	132.50	349.82	614.82	725.00	28.00
687.85	439.11	416.30	408.08	487.84	133.99	131.30	356.53	619.14	750.00	29.00
717.39	429.77	458.03	399.01	501.05	146.23	143.30	357.75	644.35	745.00	29.00
736.56	420.81	503.77	390.34	512.87	156.64	153.51	359.37	666.38	700.00	30.00
721.83	412.23	521.45	395.44	512.74	150.17	147.17	365.57	659.91	695.00	30.00
707.68	403.98	509.87	413.02	508.64	141.08	138.26	370.38	646.90	690.00	31.00
694.07	396.06	498.78	441.45	507.59	131.23	128.60	378.99	636.19	685.00	31.00

B.2 AODV End-to-End Delay Data for Model Verification

Table B.2: AODV End-to-End Delay Data for Model Verification

Run 1	Run 2	Run 3	Run 4	Mean	St Dev	Conf Int	Low CI	Up CI	Rsrch
Sd 25	Sd 128	Sd 132	Sd 150						20 Nds
0.000421	0.000415	0.000422	0.000433	0.000423	0.000008	0.000007	0.000416	0.000430	0.000420
0.000421	0.000415	0.000422	0.000433	0.000423	0.000008	0.000007	0.000416	0.000430	0.000420
0.000421	0.000415	0.000422	0.000433	0.000423	0.000007	0.000007	0.000416	0.000430	0.000420
0.000421	0.000418	0.000423	0.000435	0.000424	0.000007	0.000007	0.000417	0.000431	0.000420
0.000421	0.000416	0.000426	0.000433	0.000424	0.000007	0.000007	0.000417	0.000431	0.000420
0.000421	0.000426	0.000423	0.000433	0.000426	0.000005	0.000005	0.000421	0.000431	0.000420
0.000421	0.000425	0.000423	0.000434	0.000426	0.000006	0.000006	0.000420	0.000431	0.000420
0.000421	0.000424	0.000421	0.000434	0.000425	0.000006	0.000006	0.000419	0.000431	0.000420
0.000421	0.000424	0.00042	0.000432	0.000424	0.000005	0.000005	0.000419	0.000430	0.000420
0.000424	0.000424	0.00042	0.000431	0.000425	0.000005	0.000005	0.000420	0.000429	0.000420
0.000425	0.000424	0.00042	0.000431	0.000425	0.000005	0.000004	0.000420	0.000429	0.000420
0.000425	0.000424	0.00042	0.000431	0.000425	0.000005	0.000004	0.000420	0.000429	0.000420
0.000425	0.000424	0.00042	0.000431	0.000425	0.000005	0.000004	0.000420	0.000429	0.000420
0.000424	0.000424	0.00042	0.000431	0.000425	0.000005	0.000004	0.000420	0.000429	0.000420
0.000426	0.000423	0.00042	0.000431	0.000425	0.000005	0.000005	0.000420	0.000430	0.000420
0.000428	0.000424	0.00042	0.000431	0.000426	0.000005	0.000005	0.000421	0.000431	0.000420
0.000425	0.000419	0.000421	0.000431	0.000424	0.000005	0.000005	0.000419	0.000429	0.000420
0.000425	0.000419	0.000422	0.000434	0.000425	0.000006	0.000006	0.000419	0.000431	0.000420
0.000425	0.000419	0.000421	0.000433	0.000424	0.000006	0.000006	0.000418	0.000430	0.000420
0.000424	0.000419	0.000421	0.000436	0.000425	0.000008	0.000007	0.000418	0.000433	0.000420
0.00043	0.00042	0.000421	0.000436	0.000427	0.000008	0.000007	0.000420	0.000435	0.000420
0.000428	0.000425	0.00042	0.000438	0.000428	0.000008	0.000007	0.000420	0.000435	0.000420
0.000428	0.000424	0.00042	0.000438	0.000427	0.000008	0.000008	0.000420	0.000435	0.000420
0.000428	0.000422	0.000422	0.000438	0.000428	0.000007	0.000007	0.000420	0.000435	0.000420
0.000427	0.000422	0.000424	0.000438	0.000428	0.000007	0.000007	0.000421	0.000435	0.000420
0.000427	0.000422	0.000424	0.000438	0.000428	0.000007	0.000007	0.000421	0.000435	0.000420
0.000427	0.000422	0.00042	0.000438	0.000427	0.000008	0.000008	0.000419	0.000435	0.000420
0.000427	0.000422	0.00042	0.000438	0.000427	0.000008	0.000008	0.000419	0.000435	0.000420
0.000427	0.000422	0.00042	0.000438	0.000427	0.000008	0.000008	0.000419	0.000435	0.000420
0.000427	0.000422	0.00042	0.000438	0.000427	0.000008	0.000008	0.000419	0.000435	0.000420
0.000427	0.000422	0.00042	0.000439	0.000427	0.000008	0.000008	0.000419	0.000436	0.000420
0.000427	0.000422	0.00042	0.000437	0.000427	0.000008	0.000007	0.000419	0.000434	0.000420
0.000427	0.000422	0.00042	0.000437	0.000426	0.000007	0.000007	0.000419	0.000434	0.000420
0.000427	0.000421	0.00042	0.000437	0.000426	0.000008	0.000008	0.000419	0.000434	0.000420
0.000427	0.000421	0.00042	0.000437	0.000426	0.000008	0.000008	0.000419	0.000434	0.000420
0.000425	0.000421	0.00042	0.000436	0.000426	0.000007	0.000007	0.000419	0.000433	0.000420
0.000425	0.000421	0.00042	0.000435	0.000426	0.000007	0.000007	0.000419	0.000432	0.000420
0.000424	0.000422	0.00042	0.000435	0.000425	0.000007	0.000007	0.000419	0.000432	0.000420
0.000424	0.000421	0.00042	0.000435	0.000425	0.000007	0.000007	0.000418	0.000432	0.000420
0.000423	0.000422	0.00042	0.000435	0.000425	0.000007	0.000007	0.000419	0.000432	0.000420
0.000423	0.000422	0.00042	0.000435	0.000425	0.000007	0.000007	0.000418	0.000432	0.000420
0.000423	0.000422	0.00042	0.000435	0.000425	0.000007	0.000007	0.000418	0.000432	0.000420
0.000423	0.000422	0.00042	0.000435	0.000425	0.000007	0.000007	0.000418	0.000432	0.000420

B.3 1 Feedback Node Determination Data

Table B.3: 1 Feedback Node Determination Data

1 Node	Rte Errors	Load	Throughput
1,026.00	407.18	14,039,101.36	4,160,498.75
1,053.00	406.43	14,039,007.38	4,191,310.93
1,080.00	408.85	14,040,683.68	4,154,922.35
1,107.00	407.67	14,032,248.49	4,112,905.11
1,134.00	407.72	14,033,340.28	4,106,857.87
1,161.00	407.68	14,034,537.27	4,077,854.90
1,188.00	409.18	14,039,265.45	4,061,493.62
1,215.00	410.09	14,043,582.25	4,041,508.35
1,242.00	409.36	14,046,652.37	4,025,698.52
1,269.00	409.63	14,051,550.96	4,031,726.12
1,296.00	410.14	14,052,585.82	4,045,482.93
1,323.00	409.96	14,061,492.88	4,063,179.14
1,350.00	406.39	14,065,305.89	4,098,668.78
1,377.00	401.69	14,060,206.43	4,134,066.42
1,404.00	396.28	14,043,507.21	4,179,255.77
1,431.00	392.22	14,038,809.74	4,218,635.39
1,458.00	396.00	14,055,078.64	4,221,272.20
1,485.00	394.80	14,068,858.56	4,245,317.54
1,512.00	394.19	14,070,348.93	4,254,493.75
1,539.00	395.33	14,072,666.09	4,217,974.23
1,566.00	402.22	14,093,438.23	4,189,199.59
1,593.00	404.13	14,090,859.85	4,151,944.36
1,620.00	406.20	14,100,143.64	4,122,423.14
1,647.00	408.34	14,102,742.16	4,093,958.50
1,674.00	408.33	14,110,949.96	4,105,445.04
1,701.00	408.13	14,115,988.24	4,123,198.80
1,728.00	406.45	14,114,193.19	4,138,973.94
1,755.00	404.33	14,112,814.46	4,159,341.40
1,782.00	401.99	14,111,693.48	4,185,688.15
1,809.00	401.78	14,108,929.34	4,178,652.71
1,836.00	402.86	14,111,499.95	4,175,560.98
1,863.00	404.27	14,118,423.50	4,174,904.91
1,890.00	405.46	14,120,327.14	4,149,313.25
1,917.00	410.81	14,137,504.31	4,132,230.35
1,944.00	414.08	14,145,215.40	4,110,779.06
1,971.00	414.80	14,146,448.34	4,080,127.23
1,998.00	420.43	14,166,064.34	4,064,495.64
2,025.00	430.93	14,198,166.18	4,064,212.94
2,052.00	432.08	14,197,254.93	4,059,751.13
2,079.00	431.46	14,192,569.75	4,069,507.40
2,106.00	436.01	14,206,631.40	4,053,096.66
2,133.00	434.35	14,200,575.02	4,029,663.72
2,160.00	432.94	14,194,091.34	4,003,018.42
2,187.00	430.98	14,187,423.42	3,974,987.81
2,214.00	433.16	14,193,377.03	3,958,206.66
2,241.00	433.65	14,197,733.05	3,940,961.16
2,268.00	433.82	14,198,890.16	3,931,597.93
2,295.00	433.52	14,196,843.89	3,918,702.55
2,322.00	434.20	14,199,765.96	3,904,046.47
2,349.00	432.33	14,192,127.87	3,886,868.88
2,376.00	432.30	14,196,897.58	3,872,766.63
2,403.00	432.28	14,194,287.16	3,849,363.21
2,430.00	430.95	14,190,752.49	3,825,585.01
2,457.00	432.28	14,192,651.13	3,809,312.97
2,484.00	436.55	14,207,541.45	3,801,849.51
2,511.00	437.76	14,212,729.09	3,806,244.64
2,538.00	434.16	14,204,124.92	3,835,185.98
2,565.00	434.48	14,202,373.85	3,826,977.85
2,592.00	431.68	14,199,275.12	3,832,204.13
2,619.00	430.34	14,201,775.37	3,846,815.11
2,646.00	429.56	14,199,558.32	3,837,042.20
2,673.00	430.14	14,198,773.21	3,827,005.33

B.4 2 Feedback Node Determination Data

Table B.4: 2 Feedback Nodes Determination Data

2 Nodes	Rte Errors	Load	Throughput
1,026.00	376.59	13,567,119.68	2,393,728.09
1,053.00	376.50	13,592,020.39	2,467,927.20
1,080.00	375.76	13,606,490.91	2,531,434.26
1,107.00	379.36	13,628,046.93	2,586,120.95
1,134.00	383.21	13,646,365.88	2,626,244.02
1,161.00	384.55	13,660,809.62	2,635,542.03
1,188.00	388.78	13,679,866.26	2,638,062.78
1,215.00	389.41	13,693,396.82	2,672,385.91
1,242.00	386.34	13,689,562.02	2,743,385.75
1,269.00	388.23	13,699,446.30	2,768,128.05
1,296.00	387.69	13,709,782.18	2,819,577.11
1,323.00	388.48	13,720,483.25	2,863,426.11
1,350.00	384.84	13,726,281.60	2,929,614.32
1,377.00	386.62	13,740,162.10	2,954,656.00
1,404.00	387.70	13,745,020.53	2,939,939.80
1,431.00	393.80	13,775,505.16	2,941,807.80
1,458.00	395.71	13,787,341.47	2,934,059.85
1,485.00	395.95	13,790,425.42	2,926,514.75
1,512.00	395.40	13,796,100.97	2,945,083.90
1,539.00	394.07	13,798,492.40	2,956,023.42
1,566.00	395.10	13,803,061.88	2,941,220.18
1,593.00	395.05	13,805,877.59	2,929,923.99
1,620.00	394.59	13,806,730.65	2,918,442.65
1,647.00	394.87	13,816,663.13	2,925,149.34
1,674.00	396.79	13,822,955.89	2,924,261.08
1,701.00	398.33	13,830,598.43	2,939,284.15
1,728.00	394.51	13,825,305.98	2,990,841.38
1,755.00	393.02	13,828,801.60	3,021,398.88
1,782.00	390.91	13,831,686.26	3,061,530.46
1,809.00	393.85	13,841,416.89	3,084,569.36
1,836.00	394.54	13,844,388.57	3,108,012.95
1,863.00	395.50	13,852,525.95	3,112,366.17
1,890.00	402.89	13,877,269.57	3,114,858.90
1,917.00	404.64	13,886,041.09	3,106,713.51
1,944.00	408.67	13,902,414.90	3,102,630.11
1,971.00	410.55	13,910,621.10	3,094,295.35
1,998.00	413.15	13,921,590.93	3,086,365.63
2,025.00	412.89	13,924,390.91	3,079,802.93
2,052.00	416.04	13,940,633.89	3,082,540.30
2,079.00	418.53	13,953,390.86	3,098,086.67
2,106.00	417.32	13,959,597.91	3,129,304.69
2,133.00	417.36	13,967,518.56	3,152,700.28
2,160.00	416.57	13,972,739.15	3,180,754.79
2,187.00	416.83	13,976,169.26	3,176,712.96
2,214.00	417.73	13,981,100.71	3,184,647.60
2,241.00	418.43	13,984,933.98	3,174,872.85
2,268.00	420.41	13,990,925.86	3,168,413.98
2,295.00	418.16	13,983,096.05	3,149,356.56
2,322.00	417.97	13,950,963.55	3,131,979.96
2,349.00	416.25	13,933,666.87	3,112,743.70
2,376.00	419.29	13,915,954.06	3,102,487.80
2,403.00	422.47	13,924,522.89	3,095,450.15
2,430.00	422.44	13,923,428.42	3,084,906.25
2,457.00	421.24	13,923,689.57	3,100,539.47
2,484.00	421.00	13,924,252.29	3,093,415.19
2,511.00	420.53	13,928,749.89	3,093,416.13
2,538.00	420.06	13,929,571.67	3,091,395.18
2,565.00	419.21	13,931,134.75	3,116,494.38
2,592.00	420.97	13,937,490.95	3,124,168.65
2,619.00	421.86	13,940,837.10	3,114,542.67
2,646.00	422.77	13,944,645.64	3,118,201.33
2,673.00	422.30	13,943,061.99	3,111,000.58

B.5 3 Feedback Node Determination Data

Table B.5: 3 Feedback Nodes Determination Data

3 Nodes	Rte Errors	Load	Throughput
1,026.00	376.59	13,567,119.68	2,393,728.09
1,053.00	376.50	13,592,020.39	2,467,927.20
1,080.00	375.76	13,606,490.91	2,531,434.26
1,107.00	379.36	13,628,046.93	2,586,120.95
1,134.00	383.21	13,646,365.88	2,626,244.02
1,161.00	384.55	13,660,809.62	2,635,542.03
1,188.00	388.78	13,679,866.26	2,638,062.78
1,215.00	389.41	13,693,396.82	2,672,385.91
1,242.00	386.34	13,689,562.02	2,743,385.75
1,269.00	388.23	13,699,446.30	2,768,128.05
1,296.00	387.69	13,709,782.18	2,819,577.11
1,323.00	388.48	13,720,483.25	2,863,426.11
1,350.00	384.84	13,726,281.60	2,929,614.32
1,377.00	386.62	13,740,162.10	2,954,656.00
1,404.00	387.70	13,745,020.53	2,939,939.80
1,431.00	393.80	13,775,505.16	2,941,807.80
1,458.00	395.71	13,787,341.47	2,934,059.85
1,485.00	395.95	13,790,425.42	2,926,514.75
1,512.00	395.40	13,796,100.97	2,945,083.90
1,539.00	394.07	13,798,492.40	2,956,023.42
1,566.00	395.10	13,803,061.88	2,941,220.18
1,593.00	395.05	13,805,877.59	2,929,923.99
1,620.00	394.59	13,806,730.65	2,918,442.65
1,647.00	394.87	13,816,663.13	2,925,149.34
1,674.00	396.79	13,822,955.89	2,924,261.08
1,701.00	398.33	13,830,598.43	2,939,284.15
1,728.00	394.51	13,825,305.98	2,990,841.38
1,755.00	393.02	13,828,801.60	3,021,398.88
1,782.00	390.91	13,831,686.26	3,061,530.46
1,809.00	393.85	13,841,416.89	3,084,569.36
1,836.00	394.54	13,844,388.57	3,108,012.95
1,863.00	395.50	13,852,525.95	3,112,366.17
1,890.00	402.89	13,877,269.57	3,114,858.90
1,917.00	404.64	13,886,041.09	3,106,713.51
1,944.00	408.67	13,902,414.90	3,102,630.11
1,971.00	410.55	13,910,621.10	3,094,295.35
1,998.00	413.15	13,921,590.93	3,086,365.63
2,025.00	412.89	13,924,390.91	3,079,802.93
2,052.00	416.04	13,940,633.89	3,082,540.30
2,079.00	418.53	13,953,390.86	3,098,086.67
2,106.00	417.32	13,959,597.91	3,129,304.69
2,133.00	417.36	13,967,518.56	3,152,700.28
2,160.00	416.57	13,972,739.15	3,180,754.79
2,187.00	416.83	13,976,169.26	3,176,712.96
2,214.00	417.73	13,981,100.71	3,184,647.60
2,241.00	418.43	13,984,933.98	3,174,872.85
2,268.00	420.41	13,990,925.86	3,168,413.98
2,295.00	418.16	13,983,096.05	3,149,356.56
2,322.00	417.97	13,950,963.55	3,131,979.96
2,349.00	416.25	13,933,666.87	3,112,743.70
2,376.00	419.29	13,915,954.06	3,102,487.80
2,403.00	422.47	13,924,522.89	3,095,450.15
2,430.00	422.44	13,923,428.42	3,084,906.25
2,457.00	421.24	13,923,689.57	3,100,539.47
2,484.00	421.00	13,924,252.29	3,093,415.19
2,511.00	420.53	13,928,749.89	3,093,416.13
2,538.00	420.06	13,929,571.67	3,091,395.18
2,565.00	419.21	13,931,134.75	3,116,494.38
2,592.00	420.97	13,937,490.95	3,124,168.65
2,619.00	421.86	13,940,837.10	3,114,542.67
2,646.00	422.77	13,944,645.64	3,118,201.33
2,673.00	422.30	13,943,061.99	3,111,000.58

B.6 4 Feedback Node Determination Data

Table B.6: 4 Feedback Nodes Determination Data

4 Nodes	Rte Errors	Load	Throughput
1,026.00	377.08	13,241,289.60	3,274,775.92
1,053.00	374.80	13,255,385.99	3,302,498.67
1,080.00	373.02	13,266,363.75	3,351,285.62
1,107.00	374.12	13,289,904.25	3,390,029.15
1,134.00	376.07	13,313,602.81	3,420,716.82
1,161.00	381.68	13,348,481.37	3,443,208.78
1,188.00	381.80	13,373,878.89	3,489,482.98
1,215.00	380.37	13,382,574.09	3,539,418.64
1,242.00	380.55	13,401,510.18	3,564,044.51
1,269.00	382.63	13,420,764.07	3,554,664.47
1,296.00	387.43	13,443,352.82	3,533,635.58
1,323.00	387.20	13,458,592.45	3,542,734.89
1,350.00	386.71	13,470,465.09	3,581,495.54
1,377.00	388.21	13,479,955.65	3,596,705.66
1,404.00	389.32	13,498,789.17	3,617,100.84
1,431.00	391.33	13,513,544.23	3,607,236.96
1,458.00	392.42	13,530,198.80	3,609,962.73
1,485.00	392.86	13,544,757.78	3,633,289.69
1,512.00	393.61	13,558,902.44	3,647,429.22
1,539.00	395.26	13,572,734.55	3,638,009.75
1,566.00	396.31	13,586,314.53	3,633,845.64
1,593.00	397.53	13,604,033.32	3,651,168.53
1,620.00	397.02	13,613,852.81	3,673,338.29
1,647.00	396.79	13,623,420.12	3,711,542.48
1,674.00	396.98	13,632,440.63	3,731,753.43
1,701.00	390.92	13,623,389.30	3,777,202.67
1,728.00	386.75	13,617,341.76	3,808,388.94
1,755.00	384.33	13,629,976.12	3,829,390.96
1,782.00	386.88	13,647,322.59	3,832,373.60
1,809.00	387.78	13,659,861.75	3,849,075.28
1,836.00	388.57	13,670,314.01	3,860,452.84
1,863.00	389.54	13,680,947.20	3,868,786.51
1,890.00	387.04	13,685,166.86	3,900,002.17
1,917.00	384.92	13,688,128.46	3,925,275.14
1,944.00	386.62	13,698,749.34	3,916,146.75
1,971.00	386.22	13,706,452.08	3,919,270.07
1,998.00	386.53	13,712,447.65	3,923,612.00
2,025.00	389.84	13,727,393.70	3,924,502.10
2,052.00	389.40	13,733,362.19	3,936,203.16
2,079.00	388.71	13,735,501.40	3,958,709.39
2,106.00	387.13	13,732,743.41	3,986,870.76
2,133.00	388.15	13,740,944.53	3,975,433.13
2,160.00	391.31	13,753,634.58	3,957,098.16
2,187.00	396.70	13,774,031.58	3,942,952.86
2,214.00	402.63	13,798,496.97	3,933,427.22
2,241.00	405.77	13,812,148.39	3,916,897.02
2,268.00	408.71	13,824,832.52	3,901,760.38
2,295.00	414.01	13,845,538.22	3,894,360.88
2,322.00	416.05	13,857,031.89	3,881,683.17
2,349.00	417.53	13,864,017.67	3,871,924.39
2,376.00	418.08	13,866,910.19	3,857,995.37
2,403.00	419.76	13,878,123.25	3,853,392.08
2,430.00	420.10	13,883,534.64	3,839,825.80
2,457.00	420.33	13,887,379.29	3,828,323.71
2,484.00	424.61	13,907,012.61	3,829,809.75
2,511.00	426.00	13,913,096.41	3,821,735.58
2,538.00	426.89	13,916,707.81	3,813,772.73
2,565.00	428.05	13,919,854.27	3,802,442.17
2,592.00	427.76	13,925,380.97	3,818,124.62
2,619.00	425.98	13,928,306.02	3,834,528.81
2,646.00	424.03	13,933,996.14	3,855,626.76
2,673.00	425.21	13,943,077.32	3,865,518.32

B.7 5 Feedback Node Determination Data

Table B.7: 5 Feedback Nodes Determination Data

5 Nodes	Rte Errors	Load	Throughput
1,026.00	423.87	13,367,020.67	2,455,289.47
1,053.00	425.23	13,394,745.78	2,471,883.94
1,080.00	425.07	13,416,231.92	2,479,920.07
1,107.00	425.50	13,437,250.57	2,508,185.06
1,134.00	423.09	13,455,484.72	2,568,376.61
1,161.00	420.86	13,475,877.63	2,631,256.43
1,188.00	415.80	13,484,653.83	2,703,912.24
1,215.00	421.11	13,516,208.72	2,729,402.49
1,242.00	424.53	13,538,297.19	2,726,624.23
1,269.00	426.21	13,557,478.99	2,718,272.15
1,296.00	428.71	13,579,928.84	2,734,289.71
1,323.00	426.68	13,585,313.66	2,733,916.11
1,350.00	425.45	13,596,501.50	2,732,222.26
1,377.00	428.50	13,616,034.19	2,728,985.09
1,404.00	430.00	13,632,459.32	2,723,426.33
1,431.00	430.50	13,642,030.49	2,729,529.28
1,458.00	431.29	13,654,315.57	2,737,563.30
1,485.00	431.25	13,672,720.91	2,776,353.93
1,512.00	432.56	13,691,749.63	2,801,469.57
1,539.00	432.05	13,707,141.72	2,837,728.80
1,566.00	432.10	13,718,059.51	2,878,215.85
1,593.00	431.43	13,728,178.19	2,903,986.21
1,620.00	429.03	13,737,644.43	2,952,850.34
1,647.00	428.55	13,745,885.02	2,973,714.10
1,674.00	430.41	13,756,848.01	2,984,812.44
1,701.00	429.00	13,767,625.20	3,022,096.37
1,728.00	429.09	13,779,910.09	3,035,979.12
1,755.00	427.64	13,776,373.39	3,018,415.87
1,782.00	426.91	13,779,090.95	3,006,329.31
1,809.00	431.99	13,804,813.93	3,006,694.38
1,836.00	436.28	13,823,542.54	3,004,380.51
1,863.00	439.20	13,838,862.48	3,001,000.55
1,890.00	439.76	13,846,957.69	3,008,214.44
1,917.00	436.22	13,843,128.18	3,056,121.45
1,944.00	436.38	13,851,097.88	3,073,160.12
1,971.00	432.41	13,859,841.87	3,116,878.27
1,998.00	430.96	13,863,589.61	3,125,630.06
2,025.00	431.08	13,865,128.78	3,112,459.91
2,052.00	432.84	13,874,661.16	3,107,461.42
2,079.00	432.65	13,879,041.05	3,099,021.28
2,106.00	432.73	13,883,691.97	3,092,244.69
2,133.00	433.75	13,890,239.76	3,106,422.37
2,160.00	433.14	13,892,655.70	3,130,886.77
2,187.00	432.24	13,896,647.18	3,148,230.78
2,214.00	431.29	13,903,359.49	3,174,243.47
2,241.00	431.26	13,910,540.33	3,192,000.79
2,268.00	429.36	13,906,596.02	3,223,483.84
2,295.00	427.12	13,903,968.04	3,255,476.12
2,322.00	424.55	13,902,928.57	3,287,029.81
2,349.00	424.25	13,905,419.30	3,300,742.07
2,376.00	424.22	13,906,923.92	3,301,005.84
2,403.00	423.72	13,909,071.55	3,296,880.17
2,430.00	424.51	13,913,935.33	3,292,647.70
2,457.00	427.07	13,922,666.09	3,287,126.52
2,484.00	427.57	13,925,285.35	3,292,221.08
2,511.00	427.02	13,930,768.77	3,311,804.17
2,538.00	425.35	13,931,384.66	3,338,634.37
2,565.00	423.94	13,933,482.68	3,360,147.63
2,592.00	424.10	13,939,686.37	3,371,775.29
2,619.00	422.20	13,946,195.53	3,389,368.74
2,646.00	421.57	13,950,871.33	3,406,028.02
2,673.00	421.96	13,954,567.57	3,413,766.19

Table B.8: 6 Feedback Nodes Determination Data

6 Nodes	Rte Errors	Load	Throughput
1,026.00	489.85	13,564,145.50	3,154,758.17
1,053.00	490.10	13,580,092.41	3,150,506.55
1,080.00	492.02	13,598,186.55	3,147,056.71
1,107.00	493.24	13,620,438.18	3,138,300.33
1,134.00	494.00	13,639,126.79	3,119,162.82
1,161.00	488.73	13,638,976.00	3,157,529.32
1,188.00	486.02	13,647,506.57	3,188,016.38
1,215.00	485.13	13,658,357.26	3,203,630.43
1,242.00	483.04	13,663,990.64	3,239,972.72
1,269.00	476.85	13,661,289.75	3,305,802.12
1,296.00	471.33	13,658,492.40	3,352,023.95
1,323.00	477.96	13,689,924.15	3,338,552.23
1,350.00	486.27	13,726,036.71	3,338,927.92
1,377.00	487.52	13,739,138.07	3,336,097.25
1,404.00	485.21	13,738,441.73	3,361,906.54
1,431.00	483.28	13,740,598.19	3,399,921.08
1,458.00	476.96	13,735,975.74	3,458,487.04
1,485.00	475.86	13,748,940.17	3,477,644.78
1,512.00	475.68	13,758,910.96	3,495,865.53
1,539.00	477.95	13,773,607.36	3,488,355.15
1,566.00	477.49	13,783,077.81	3,479,868.26
1,593.00	476.58	13,789,152.85	3,475,779.50
1,620.00	477.56	13,800,993.01	3,481,918.04
1,647.00	476.52	13,806,316.25	3,477,185.64
1,674.00	476.52	13,813,706.01	3,478,979.57
1,701.00	474.11	13,816,338.67	3,503,241.70
1,728.00	474.28	13,819,713.44	3,485,359.64
1,755.00	473.26	13,824,677.94	3,466,090.06
1,782.00	473.15	13,834,500.09	3,452,327.02
1,809.00	477.35	13,855,711.39	3,445,362.91
1,836.00	476.33	13,861,277.89	3,438,265.85
1,863.00	476.50	13,870,199.62	3,452,101.30
1,890.00	476.85	13,881,087.72	3,468,738.84
1,917.00	476.58	13,891,257.61	3,490,618.85
1,944.00	477.67	13,900,433.68	3,503,717.65
1,971.00	473.15	13,891,563.95	3,535,566.37
1,998.00	472.77	13,894,722.86	3,538,448.78
2,025.00	473.72	13,906,224.94	3,546,788.66
2,052.00	473.00	13,912,987.64	3,557,471.60
2,079.00	472.73	13,920,890.82	3,567,716.16
2,106.00	472.58	13,926,589.88	3,579,305.77
2,133.00	471.00	13,926,899.75	3,576,504.92
2,160.00	471.93	13,933,017.18	3,573,724.44
2,187.00	473.02	13,939,348.51	3,564,823.34
2,214.00	472.82	13,943,283.79	3,554,921.71
2,241.00	472.58	13,943,772.30	3,545,070.05
2,268.00	472.99	13,948,503.70	3,530,922.25
2,295.00	474.21	13,953,632.04	3,514,351.45
2,322.00	472.53	13,949,728.53	3,495,519.93
2,349.00	474.08	13,958,066.49	3,482,328.12
2,376.00	473.26	13,957,417.61	3,466,201.77
2,403.00	472.38	13,957,077.48	3,455,270.69
2,430.00	472.47	13,959,278.87	3,438,899.65
2,457.00	470.55	13,949,642.73	3,418,610.38
2,484.00	468.68	13,943,001.04	3,399,673.93
2,511.00	470.39	13,949,479.19	3,389,113.39
2,538.00	470.05	13,953,101.36	3,383,971.04
2,565.00	470.25	13,956,747.77	3,383,276.25
2,592.00	468.57	13,954,975.60	3,403,157.61
2,619.00	465.60	13,950,698.20	3,432,797.13
2,646.00	464.07	13,951,077.17	3,444,202.30
2,673.00	461.11	13,948,081.59	3,473,228.42

Appendix C.

The following tables contain the C.O.V. results of each simulation run.

C.1 Baseline 50 Nodes - 0 Misbehaving

Table C.1: Baseline 50 Nodes - 0 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	2.6014	2.9335	3.9505
2	-0.8076	-1.4165	3.5982
3	-0.0312	0.6659	-6.7657
4	-1.9947	-2.5362	-2.3092

C.2 Baseline 50 Nodes - 25 Misbehaving

Table C.2: Baseline 50 Nodes - 25 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-0.3196	-0.2436	-1.2804
2	-0.7252	-1.1087	2.5226
3	-0.8063	-0.9896	-8.1109
4	1.7516	2.1805	4.8477

C.3 Baseline 50 Nodes - 5 Misbehaving

Table C.3: Baseline 50 Nodes - 5 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-0.5123	-1.4171	5.5880
2	1.8942	2.7289	-4.5483
3	-1.2838	-1.1586	-5.5261
4	-0.2245	-0.4070	2.5115

C.4 RIPSec 50 Nodes - 0 Misbehaving

Table C.4: RIPSec 50 Nodes - 0 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-0.2383	1.1754	-10.3107
2	2.9627	2.6936	9.9661
3	0.3117	0.2349	1.8219
4	-3.5044	-4.7690	-7.3929

C.5 RIPSec 50 Nodes - 25 Misbehaving

Table C.5: RIPSec 50 Nodes - 25 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	3.0488	3.7423	0.2775
2	-2.5418	-3.2102	-0.4594
3	3.0145	4.1257	1.3553
4	-4.5128	-6.4458	-1.2565

C.6 RIPSec 50 Nodes - 5 Misbehaving

Table C.6: RIPSec 50 Nodes - 5 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-1.1096	-1.3872	-1.2443
2	1.1203	1.0901	3.6531
3	0.7422	1.7151	-10.0261
4	-0.8365	-1.6114	4.8362

C.7 Baseline 25 Nodes - 0 Misbehaving

Table C.7: Baseline 25 Nodes - 0 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	1.6601	1.0736	8.7410
2	-5.5787	-3.9631	-43.6998
3	2.7114	2.9981	-0.2371
4	0.3467	-0.6833	9.1311

C.8 Baseline 25 Nodes - 12 Misbehaving

Table C.8: Baseline 25 Nodes - 12 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-1.8964	-2.5563	3.8348
2	1.3918	1.5126	-0.2683
3	1.1316	1.3308	-2.7586
4	-0.7920	-0.5252	-1.3701

C.9 Baseline 25 Nodes - 2 Misbehaving

Table C.9: Baseline 25 Nodes - 2 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	1.1024	3.4608	5.8311
2	-8.1303	-7.8070	-34.0059
3	2.2324	0.5181	7.9094
4	3.1595	2.2520	2.8140

C.10 RIPSec 25 Nodes - 0 Misbehaving

Table C.10: RIPSec 25 Nodes - 0 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-0.1213	-0.3861	0.7972
2	1.0028	1.0499	3.6152
3	0.9629	1.2850	1.5863
4	-1.9722	-2.1105	-7.4544

C.11 RIPSec 25 Nodes - 12 Misbehaving

Table C.11: RIPSec 25 Nodes - 12 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-26.7139	-34.5721	-41.4710
2	-6.0982	-5.6842	-18.9739
3	20.1544	21.4738	23.5611
4	-21.6734	-26.8248	-22.4710

C.12 RIPSec 25 Nodes - 2 Misbehaving

Table C.12: RIPSec 25 Nodes - 2 Misbehaving

Run #	Load C.O.V.	Throughput C.O.V.	Errors C.O.V.
1	-1.1152	-1.9159	3.6066
2	3.0335	3.3618	6.1007
3	0.2503	0.6508	-11.1847
4	-2.5561	-2.6013	-2.1378

Bibliography

1. Adams, William Joseph, Dr. Nathaniel J. Davis Iv, Dr. Scott, F. Midkiff, Dr. William, T. Baumann, Dr. Edward, L. Green, and William J. Adams. "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration". *IEEE Workshop on Information Assurance*, 324. 2005.

2. Adams, WJ, GC Hadjichristofi, and NJ Davis IV. "Calculating a Node's Reputation in a Mobile Ad Hoc Network". *24th IEEE International Performance, Computing, and Communications Conference*, 303–307, 2005.

3. Allen, J. and B. Walsh. "Enhanced Oil Spill Surveillance; Detection and Monitoring Through the Applied Technology of Unmanned Air Systems". *2008 International Oil Spill Conference*. American Petroleum Institute, 1220 L Street, NW Washington DC 20005 USA, 2008.

4. Alshamsi, A. and T. Saito. "A Technical Comparison of IPSec and SSL". *19th International Conference on Advanced Information Networking and Applications*, volume 2. 2005.

5. America, C. "Airborne Science Newsletter". *Newsletter*, 2010.

6. Anantvalee, T. and J. Wu. "A survey on Intrusion Detection in Mobile Ad Hoc Networks". *Wireless/Mobile Network Security*, 170–196, 2006.

7. Ariza-Quintana, A., E. Casilari, and A.T. Cabrera. "Implementation of MANET Routing Protocols on OMNeT++". *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems Workshops*, 80. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2008.

8. Austin, R. *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. Wiley, 2010.

9. Bellur, B.R., M.G. Lewis, and F.L. Templin. "Tactical Information Operations for Autonomous Teams of Unmanned Aerial Vehicles (UAVs)". *IEEE Aerospace Conference Proceedings*, volume 6, 6–2741. 2002.

10. Broch, J., D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva. "A performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 85–97. Association for Computing Machinery, 1998.

11. Buchegger, S. "Performance Analysis of the CONFIDANT Protocol". *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking Computing*, 226–236, 2002.

12. Capkun, S., L. Buttyán, and J.P. Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks". *IEEE Transaction on Mobile Computing*, 52–64, 2003.

13. Carruthers, R. and I. Nikolaidis. "Certain Limitations of Reputation-Based Schemes in Mobile Environments". *Proceedings of the 8th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2–11, 2005.

14. Carvalho, M. "Security in Mobile Ad Hoc Networks". *IEEE Security & Privacy*, 72–75, 2008.

15. Chakeres, ID and EM Belding-Royer. "AODV Routing Protocol Implementation Design". *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops*, 698–703. 2004.

16. Chakrabarti, S. and A. Mishra. "QoS Issues in Ad Hoc Wireless Networks". *IEEE Communications Magazine*, 39(2):142–148, 2001.

17. Chen, N.Y.X.L.Q. and SM Emran. "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data". *IEEE Transactions on Systems, Man and Cybernetics, Part A*, 31(4):266–274, 2001.

18. Dai, W. and P. Topiwala. "SmartCapture: A Compact Video Capture, Encoding and Streaming Technology for UAVs". *Proceedings of SPIE*, volume 6946, 69460F. 2008.

19. DaSilva, LA, SF Midkiff, JS Park, GC Hadjichristofi, NJ Davis, and KS Phanse. "Network Mobility and Protocol Interoperability in Ad Hoc Networks". *Communications Magazine, IEEE*, 42(11):88–96, 2004.

20. Debar, H., M. Becker, and D. Siboni. "A Neural Network Component for an Intrusion Detection System". *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 240–250. 1992.

21. Devore, J.L. and N.R. Farnum. *Applied Statistics for Engineers and Scientists*. Thomson Brooks/Cole, 2005.

22. Doraswamy, N. and D. Harkins. *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall PTR Upper Saddle River, NJ, USA, 1999.

23. Esposito, M., C. Mazzariello, F. Oliviero, S.P. Romano, and C. Sansone. "Evaluating Pattern Recognition Techniques in Intrusion Detection Systems". *Proceedings of the 5th International Workshop on Pattern Recognition in Information Systems*, 144–153. 2005.

24. Florez, G., SA Bridges, and RB Vaughn. "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection". *Annual Meeting of the North American Fuzzy Information Processing Society*, 457–462. 2002.

25. Forrest, S. and C. Beauchemin. "Computer Immunology". *Immunological Reviews*, 216(1):176, 2007.

26. Garg, N. and RP Mahapatra. "MANET Security Issues". *International Journal of Computer Science and Network Security*, 9(8):241, 2009.

27. Georgios, K., K. Elisavet, D. Anastasia, A. Marios, and F. Georgios. "Efficient Certification Path Discovery for MANET". *EURASIP Journal on Wireless Communications and Networking*, 2010.

28. Gonner, R., D. Schatzmann, B. Plattner, et al. "Evaluation of Scheduling Methods over Multipath Routing in Wireless Mobile Ad Hoc Networks". *Semester Thesis, Institute for Technology, Zurich, Germany, SA-2006-26*, 2006.

29. Grandison, T.W.A. *Trust Management for Internet Applications*. Ph.D. thesis, Imperial College, 2003.

30. Guide, J.M.P.S. "Version 4". *Arxiv Preprint Physics/0703039 (http://arxiv.org/abs/physics/0703039)*, 2009.

31. Hadjichristofi, G.C. *A Framework for Providing Redundancy and Robustness in Key Management for IPSec Security Associations in a Mobile Ad Hoc Environment*. Ph.D. thesis, Virginia Polytechnic Institute and State University, 2005.

32. Houser, D. and J. Wooders. "Reputation in Auctions: Theory and Evidence from eBay". *Journal of Economics & Management Strategy*, 15(2):353–369, 2006.

33. Hu, Y.C., D.B. Johnson, and A. Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks". *Ad Hoc Networks*, 1(1):175–192, 2003.

34. Hu, Y.C., A. Perrig, and D.B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks". *Wireless Networks*, 11(1-2):38, 2005.

35. IRTF, RRG. "Ad Hoc Network Scaling Research Subgroup". *Notes on Scalability of Wireless Ad Hoc Networks*, 1, 2003.

36. Jain, R. *The Art of Computer Systems Performance Analysis*. Wiley New York, 1991.

37. Jang, H.C., Y.N. Lien, and T.C. Tsai. "Rescue Information System for Earthquake Disasters Based on MANET Emergency Communication Platform". *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, 623–627. Association for Computing Machinery, 2009.

38. Johansson, E. and P. Johnson. "Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition". *Proc. of CSER*, 5, 2005.

39. Johnson, D.B., D.A. Maltz, J. Broch, et al. "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks". *Ad Hoc Networking*, 5:139–172, 2001.

40. Kachirski, O. and R. Guha. "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks". *Proceedings of the IEEE Workshop on Knowledge Media Networking*, 153. IEEE Computer Society Washington, DC, USA, 2002.

41. Karygiannis, T. and L. Owens. "Wireless Network Security". *NIST Special Publication*, 800–48, 2002.

42. Kent, S. and R. Atkinson. "RFC2401: Security Architecture for the Internet Protocol". *RFC Editor United States*, 1998.

43. Ko, C., P. Brutch, J. Rowe, G. Tsafnat, and K. Levitt. "System Health and Intrusion Monitoring Using a Hierarchy of Constraints". *Lecture Notes in Computer Science*, 190–204, 2001.

44. Kolodzy, P. and K. Consulting. "MANET Gateways: Radio Interoperability Via the Internet, Not the Radio". *IEEE Communications Magazine*, 51, 2008.

45. Kumar, S.A. "Classification and Review of Security Schemes in Mobile Computing". *Wireless Sensor Network*, 2010.

46. Kumar, Sandeep and Eugene H. Spafford. "A Pattern Matching Model for Misuse Intrusion Detection". *Proceedings of the 17th National Computer Security Conference*, 11–21. 1994.

47. Kurkowski, S., T. Camp, and M. Colagrosso. "Manet Simulation Studies: The Incredibles". *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(4):61, 2005.

48. Lee, S.J. and M. Gerla. "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks". *IEEE International Conference on Communications*, 10, 2001.

49. Lee, W., SJ Stolfo, and KW Mok. "A data Mining Framework for Building Intrusion Detection Models". *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, 120–132. 1999.

50. Li, X., J. Slay, and S. Yu. "Evaluating Trust in Mobile Ad Hoc Networks". *The Workshop of International Conference on Computational Intelligence and Security*, 2005.

51. Lin, J.C., C.T. Chang, and W.T. Chung. "Design, Implementation and Performance Evaluation of IP-VPN". *17th International Conference on Advanced Information Networking and Applications*, 2003.

52. Lu, B. "Security in Mobile Ad Hoc Networks". *Handbook of Research on Wireless Security*, 2008.

53. Lunt, TF, R. Jagannathan, R. Lee, S. Listgarten, DL Edwards, HS Javitz, et al. "IDES: the Enhanced Prototype EA Real-Time Intrusion Detection Expert System Number SRI-CSL-88-12. Menlo Park". *CA: Computer Science Laboratory, SRI International*, 1988.

54. Michiardi, P. and R. Molva. "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation". *Proc. 6th IFIP CMS Conf*, 102–121, 2002.

55. Mueller, S., R.P. Tsang, and D. Ghosal. "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges". *Lecture Notes in Computer Science*, 209–234, 2004.

56. Mundinger, J. and J.Y. Le Boudec. "Analysis of a Reputation System for Mobile Ad Hoc Networks with Liars". *Performance Evaluation*, 65(3-4):212–226, 2008.

57. Neter, J., W. Wasserman, M.H. Kutner, et al. *Applied Linear Statistical Models*. Irwin Burr Ridge, Illinois, 1985.

58. Ngadi, M., A.H. Abdullah, and S. Mandala. "A survey on MANET intrusion detection". *The International Journal of Computer Science and Security*, 2(1):1–11, 2008.

59. Nichols, R.K. and P.C. Lekkas. *Wireless Security: Models, Threats, and Solutions*. McGraw-Hill Professional, 2002.

60. Nyirenda, B. *Performance Evaluation of Routing Protocols in Mobile Ad Hoc Networks (MANETs)*. Master's thesis, Blekinge Institute of Technology, 2009.

61. Oguchi, M. and M. Kamada. "Creation and Management Method of a Secure Connection on MANET Using Multi-hop Routing Protocols". *Proc. Vehicleto-Vehicle Communications 2007 (V2VCOM2007) in conjunction with IEEE Intelligent Vehicles Symposium 2007 (IV2007)*, 93–99. 2007.

62. Oh, S.Y. and M. Gerla. "Adaptive Forwarding Rate Control for Network Coding in the Tactical MANET". *Annual Conference of ITA (ACITA)*. 2009.

63. Papadimitratos, P. and Z.J. Haas. "Secure Routing for Mobile Ad Hoc Networks". *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, volume 31. IEEE, 2002.

64. Paterson, K.G. "A Cryptographic Tour of the IPSec Standards". *Information Security Technical Report*, 11(2):72–81, 2006.

65. Pham, PP and S. Perreau. "Performance Analysis of Reactive Shortest Path and Multipath Routing Mechanism with Load Balance". *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 1. 2003.

66. Porras, PA and RA Kemmerer. "Penetration State Transition Analysis: A Rule-Based Intrusion Detection Approach". *Proceedings of the Eighth Annual Computer Security Applications Conference*, 220–229. 1992.

67. Porras, P.A. and A. Valdes. "Live Traffic Analysis of TCP/IP Gateways". *Networks and Distributed Systems Security Symposium*. 1998.

68. Ramrekha, T.A. and C. Politis. "An Adaptive QoS Routing Solution for MANET Based Multimedia Communications in Emergency Cases". *Mobile Lightweight Wireless Systems*, 74–84, 2009.

69. Ramsey, F.L. and D.W. Schafer. *The Statistical Sleuth*. Duxbury/Thomson Learning, 2002.

70. Reidt, S. and S.D. Wolthusen. "Exploiting UAVs Capabilities in Tactical MANETS". *Proceedings of the 2nd Annual Conference of ITA (AC-ITA08)*, 322–323. 2008.

71. Rizvi, S.S., M.A. Jafri, K. Elleithy, and A. Riasat. "A Novel Optimization of the Distance Source Routing (DSR) Protocol for the Mobile Ad Hoc Networks (MANET)". *Novel Algorithms and Techniques in Telecommunications and Networking*, 269–274, 2010.

72. Sager, J. and Naval War Coll Newport RI Joint Military Operations Dept. *UAVs for the Operational Commander: Don't Ground Manned Aerial Vehicles (MAVs)!* Technical report, Naval War College, 2009.

73. Sánchez-Chaparro, F., J. Sierra, O. Delgado-Mohatar, and A. Fúster-Sabater. "Testing Topologies for the Evaluation of IPSEC Implementations". *Computational Science and Its Applications*, 145–154, 2009.

74. Service, German Meteorological. "IPSec Feasibility Study". *European Centre for Medium-Range Forecasts*, 2003.

75. Siddique, M.M. and A. Konsgen. "WLAN Lab OPNET Tutorial", 2007.

76. Sotirov, A., M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D.A. Osvik, and B. de Weger. "MD5 Considered Harmful Today". *Announced at the 25th Chaos Communication Congress. URL: http://www. win. tue. nl/hashclash/rogue-ca*. 2008.

77. Stallings, W. *Cryptography And Network Security: Principles and Practice*. Prentice Hall, 2006.

78. Sun, J.Z. "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing". *MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu*, 4500, 2001.

79. Super, K. and J.M. Smith. "XenITH: Xen In The Hand". *Technical Reports (CIS)*, 932, 2010.

80. Tan, K.M.C., K.S. Killourhy, and R.A. Maxion. "Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits". *LECTURE NOTES IN COMPUTER SCIENCE*, 54–73, 2002.

81. Triplett, J.E., Air Force Inst of Tech Wright-Patterson AFB OH Graduate School of Engineering, and Management. "The Effects of Commercial Video

Game Playing: A Comparison of Skills and Abilities for the Predator UAV". *Thesis*, 2008.

82. Vaidya, B. and H. Lim. "Secure Framework for Multipath Multimedia Streaming Over Wireless Ad Hoc Network". *Proceedings of the 2009 IEEE Conference on Wireless Communications & Networking Conference*, 2678–2683. IEEE, 2009.

83. Wang, L., L. Zhang, Y. Shu, and M. Dong. "Multipath Source Routing in Wireless Ad Hoc Networks". *2000 Canadian Conference on Electrical and Computer Engineering*, volume 1. 2000.

84. Wu, B., J. Chen, J. Wu, and M. Cardei. "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks". *Wireless/Mobile Network Security*, 2008.

85. Xiao, Y. "Accountability for Wireless LANs, Ad Hoc Networks, and Wireless Mesh Networks". *IEEE Communications Magazine*, 46(4):116, 2008.

86. Yang, H., H. Luo, F. Ye, S. Lu, and L. Zhang. "Security in Mobile Ad Hoc Networks: Challenges and Solutions". *IEEE Wireless Communications*, 11(1):38–47, 2004.

87. Yang, H., H. Luo, F. Ye, S. Lu, L. Zhang, and L.A. UCLA. "Security in Mobile Ad Hoc Networks: Challenges and Solutions". *IEEE Wireless Communications*, 11(1):38–47, 2004.

88. Yang, H., X. Meng, and S. Lu. "Self-Organized Network-Layer Security in Mobile Ad Hoc Networks". *Proceedings of the 1st ACM workshop on Wireless Security*, 20. ACM, 2002.

89. Yau, P. and CJ Mitchell. "Security Vulnerability in Ad Hoc Networks". *Proceedings of the 7th International Symposium on Communication Theory and Applications*, 2003.

90. Yi, S. and R. Kravets. "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks". *Pre-Proceedings of the 2nd Annual PKI Research Workshop*, volume 51, 65. 2003.

91. Yi, S., P. Naldurg, and R. Kravets. "Security-Aware Ad Hoc Routing for Wireless Networks". *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, 302. ACM, 2001.

92. Zhou, L. and ZJ Haas. "Securing Ad Hoc Networks". *IEEE Networks*, 13(6):24–30, 1999.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
16-09-2010	**Doctoral Dissertation**	Feb 2004 --- Sep 2010

4. TITLE AND SUBTITLE

Reputation-Based Internet Protocol Security: A Multilayer Security Framework For Mobile Ad Hoc Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lacey, Timothy, H.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/DCS/ENG/10-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

intentionally left blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research effort examines the theory, application, and results for a Reputation-based Internet Protocol Security (RIPSec) framework that provides security for an ad-hoc network operating in a hostile environment. In RIPSec, protection from external threats is provided in the form of encrypted communication links and encryption-wrapped nodes while internal threats are mitigated by behavior grading that assigns reputations to nodes based on their demonstrated participation in the routing process. Network availability is provided by behavior grading and round-robin multipath routing.

If a node behaves faithfully, it earns a positive reputation over time. If a node misbehaves, it earns a negative reputation. Each member of the MANET has its own unique and subjective set of Reputation Indexes (RI) that enumerates the perceived reputation of the other MANET nodes. Nodes that desire to send data will eliminate relay nodes they perceive to have a negative reputation during the formulation of a route.

A 50-node MANET is simulated with streaming multimedia and varying levels of misbehavior to determine the impact of the framework on network performance. Analysis of the simulation data shows the number of errors sent is reduced by an average of 52% when using RIPSec.

15. SUBJECT TERMS
ad hoc networks, behavior grading, IPSec, multipath routing, MANET, multilevel

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Robert F. Mills, Ph.D.
U	**U**	**U**	UU	127	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565 x4251 robert.mills@afit.edu